

# PEAP under Cisco Unified Wireless Networks with ACS 4.0 and Windows 2003

Document ID: 72013

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Network Diagram
- Conventions

#### Windows Enterprise 2003 Setup with IIS, Certificate Authority, DNS, DHCP (DC\_CA)

DC\_CA (wirelessdemoca)

#### Windows Standard 2003 Setup with Cisco Secure ACS 4.0

- Basic Installation and Configuration
- Cisco Secure ACS 4.0 Installation

#### Cisco LWAPP Controller Configuration

Create the Necessary Configuration for WPAv2/WPA

#### PEAP Authentication

- Install the Certificate Templates Snap-in
- Create the Certificate Template for the ACS Web Server
- Enable the New ACS Web Server Certificate Template

#### ACS 4.0 Certificate Setup

- Configure Exportable Certificate for ACS
- Install the Certificate in ACS 4.0 Software

#### CLIENT Configuration for PEAP using Windows Zero Touch

- Perform a Basic Installation and Configuration
- Install the Wireless Network Adapter
- Configure the Wireless Network Connection
- Problem: Odyssey Client Prompts Three Times for Token Authentication Platform
- PEAP Authentication Fails with ACS Server

#### Related Information

## Introduction

This document describes how to configure secure wireless access using Wireless LAN controllers, Microsoft Windows 2003 software and Cisco Secure Access Control Server (ACS) 4.0 via Protected Extensible Authentication Protocol (PEAP) with Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) version 2.

**Note:** For information about the deployment of secure wireless, refer to the Microsoft Wi-Fi web site and Cisco SAFE Wireless Blueprint.

## Prerequisites

### Requirements

There is an assumption that the installer has knowledge of basic Windows 2003 installation and Cisco controller installation as this document only covers the specific configurations to facilitate the tests.

For initial installation and configuration information for the Cisco 4400 Series Controllers, refer to the Quick Start Guide: Cisco 4400 Series Wireless LAN Controllers. For initial installation and configuration information for the Cisco 2000 Series Controllers, refer to the Quick Start Guide: Cisco 2000 Series Wireless LAN Controllers.

Microsoft Windows 2003 installation and configuration guides can be found at Installing Windows Server 2003 R2 .

Before you begin, install the Microsoft Windows Server 2003 with SP1 operating system on each of the servers in the test lab and update all Service Packs. Install the controllers and lightweight access points (LAPs) and ensure that the latest software updates are configured.

**Important:** At the time of this writing, SP1 is the latest Microsoft Windows Server 2003 update, and SP2 with update patches is the latest software for Microsoft Windows XP Professional.

Windows Server 2003 with SP1, Enterprise Edition, is used so that autoenrollment of user and workstation certificates for PEAP authentication can be configured. Certificate autoenrollment and autorenewal make it easier to deploy certificates and improve security by automatically expiring and renewing certificates.

## Components Used

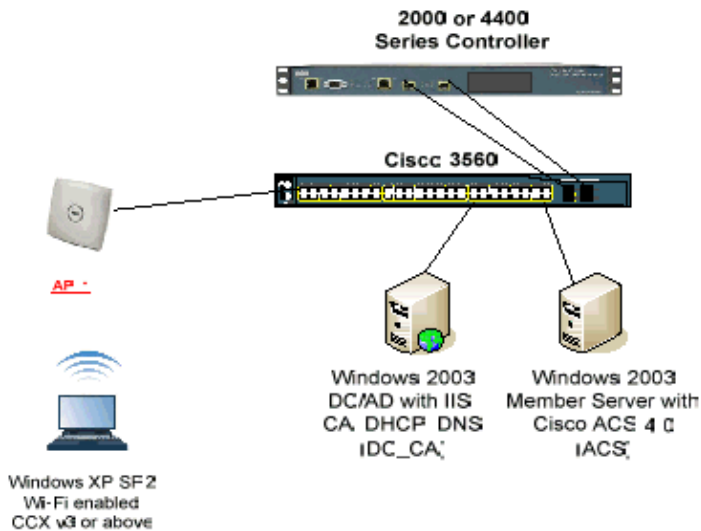
The information in this document is based on these software and hardware versions:

- Cisco 2006 or 4400 Series Controller that runs 3.2.116.21
- Cisco 1131 Lightweight Access Point Protocol (LWAPP) AP
- Windows 2003 Enterprise with Internet Information Server (IIS), Certificate Authority (CA), DHCP, and Domain Name System (DNS) installed
- Windows 2003 Standard with Access Control Server (ACS) 4.0
- Windows XP Professional with SP (and updated Service Packs) and wireless network interface card (NIC) (with CCX v3 support) or third party supplicant.
- Cisco 3560 Switch

## Network Diagram

This document uses this network setup:

### Cisco Secure Wireless Lab Topology



The primary purpose of this document is to provide you the step-by-step procedure to implement the PEAP under Unified Wireless Networks with ACS 4.0 and the Windows 2003 Enterprise server. The main emphasis is on auto-enrollment of the client so that the client auto-enrolls and takes the certificate from the server.

**Note:** In order to add Wi-Fi Protected Access (WPA)/WPA2 with Temporal Key Integrity Protocol (TKIP)/Advanced Encryption Standard (AES) to Windows XP Professional with SP, refer to WPA2/Wireless Provisioning Services Information Element (WPS IE) update for Windows XP with Service Pack 2 .

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

## Windows Enterprise 2003 Setup with IIS, Certificate Authority, DNS, DHCP (DC\_CA)

### DC\_CA (wirelessdemoca)

DC\_CA is a computer that runs Windows Server 2003 with SP1, Enterprise Edition, and performs these roles:

- A domain controller for the **wirelessdemo.local** domain that runs IIS
- A DNS server for the **wirelessdemo.local** DNS domain
- A DHCP server
- Enterprise root CA for the **wirelessdemo.local** domain

Complete these steps in order to configure DC\_CA for these services:

1. Perform a basic installation and configuration.
2. Configure the computer as a domain controller.

3. Raise the domain functional level.
4. Install and configure DHCP.
5. Install certificate services.
6. Verify Administrator permissions for certificates.
7. Add computers to the domain.
8. Allow wireless access to computers.
9. Add users to the domain.
10. Allow wireless access to users.
11. Add groups to the domain.
12. Add users to the WirelessUsers group.
13. Add client computers to the WirelessUsers group.

## **Step 1: Perform Basic Installation and Configuration**

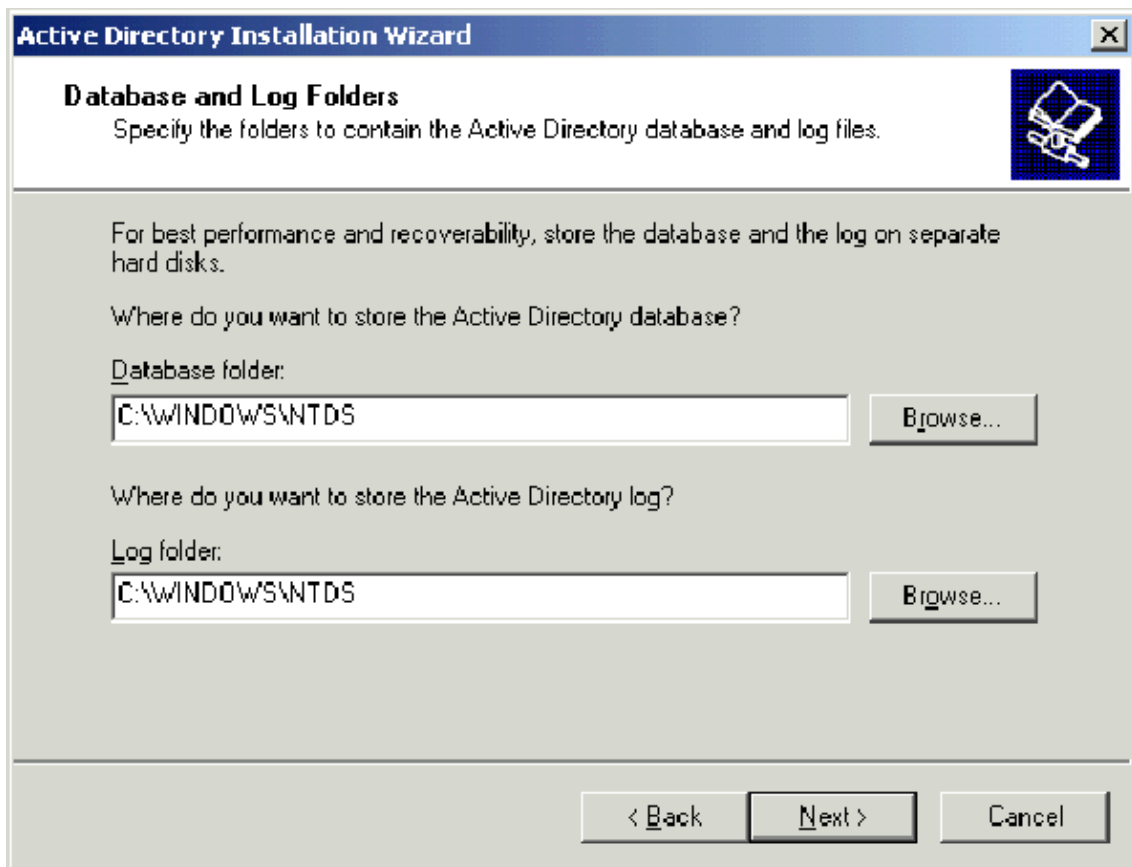
Complete these steps:

1. Install Windows Server 2003 with SP1, Enterprise Edition, as a stand-alone server.
2. Configure the TCP/IP protocol with the IP address of **172.16.100.26** and the subnet mask of **255.255.255.0**.

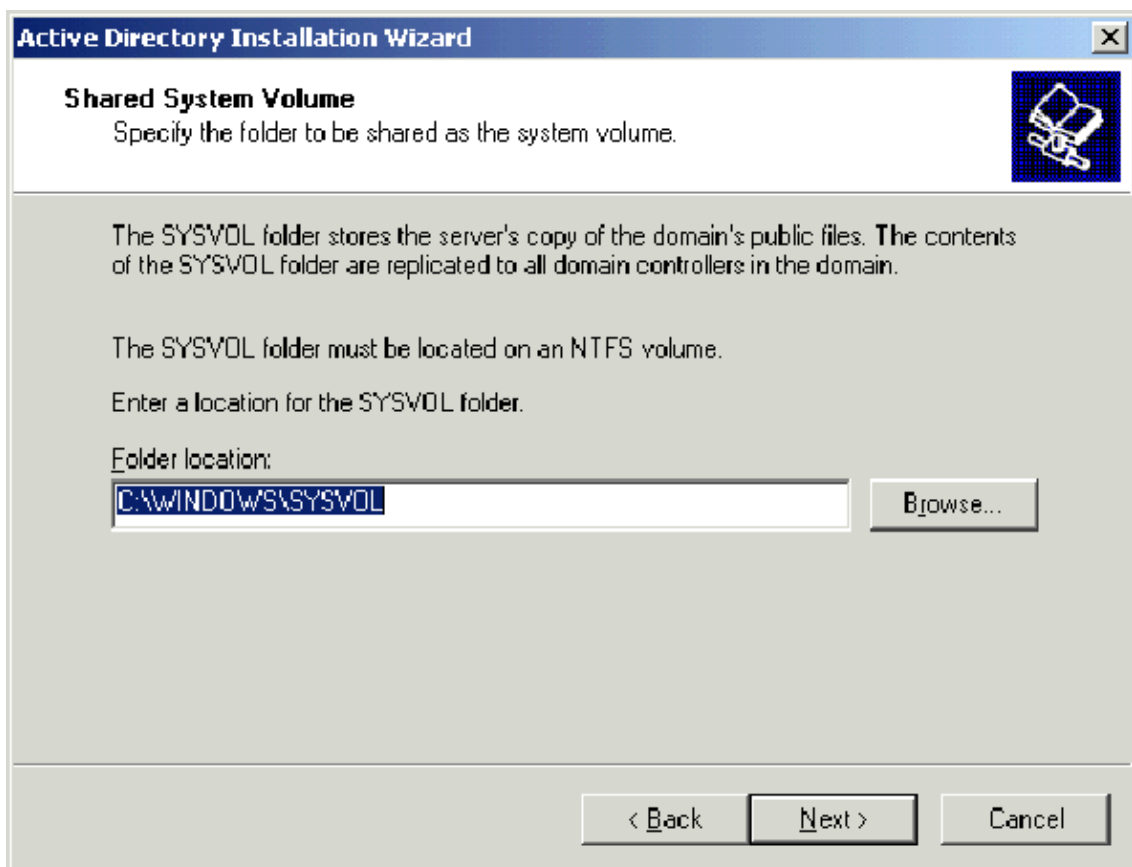
## **Step 2: Configure the Computer as a Domain Controller**

Complete these steps:

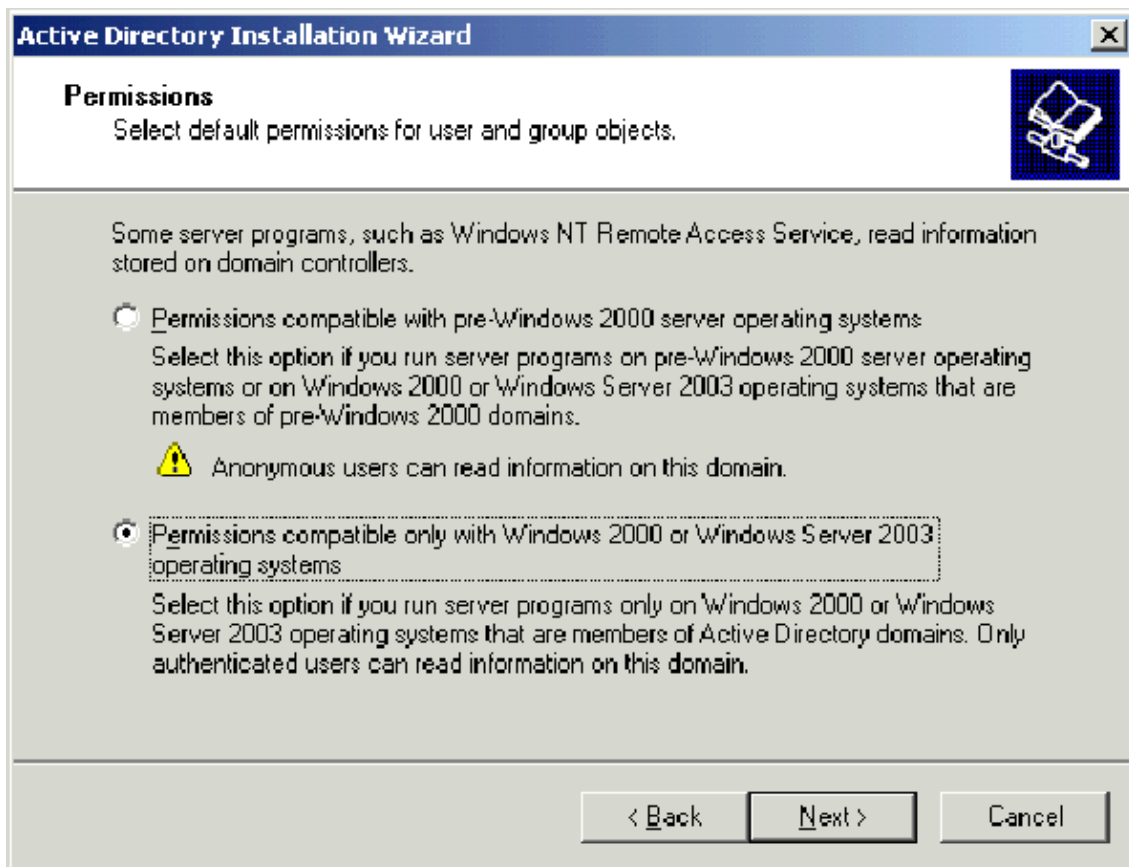
1. In order to start the Active Directory Installation wizard, choose **Start > Run**, type **dcpromo.exe**, and click **OK**.
2. On the Welcome to the Active Directory Installation Wizard page, click **Next**.
3. On the Operating System Compatibility page, click **Next**.
4. On the Domain Controller Type page, select **Domain Controller for a new Domain** and click **Next**.
5. On the Create New Domain page, select **Domain in a new forest** and click **Next**.
6. On the Install or Configure DNS page, select **No, just install and configure DNS on this computer** and click **Next**.
7. On the New Domain Name page, type **wirelessdemo.local** and click **Next**.
8. On the NetBIOS Domain Name page, enter the Domain NetBIOS name as **wirelessdemo** and click **Next**.
9. In the Database and Log Folders Locations page, accept the default Database and Log Folders directories and click **Next**.



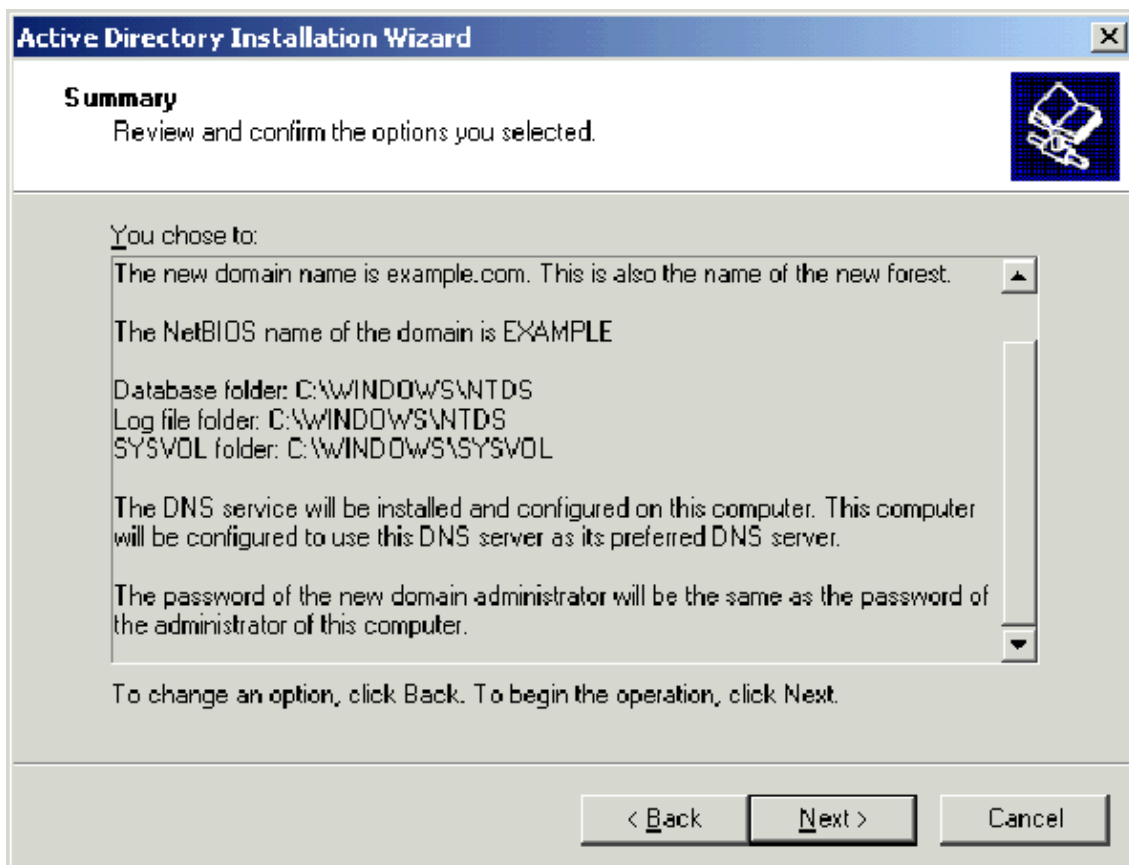
10. In the Shared System Volume page, verify that the default folder location is correct and click **Next**.



11. On the Permissions page, verify that **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems** is selected and click **Next**.



12. On the Directory Services Restore Mode Administration Password page, leave the password boxes blank and click **Next**.
13. Review the information on the Summary page and click **Next**.



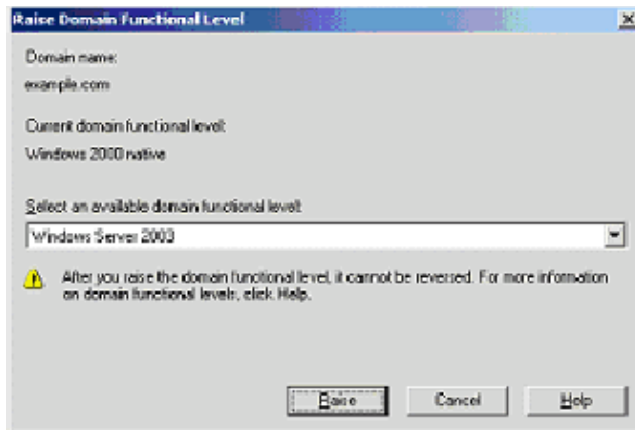
14. When you are done with the Active Directory installation, click **Finish**.

15. When prompted to restart the computer, click **Restart Now**.

### Step 3: Raise the Domain Functional Level

Complete these steps:

1. Open the **Active Directory Domains and Trusts** snap-in from the **Administrative Tools** folder (**Start > Programs > Administrative Tools > Active Directory Domains and Trusts**), and then right-click the domain computer **DC\_CA.wirelessdemo.local**.
2. Click **Raise Domain Functional Level**, and then select **Windows Server 2003** on the Raise Domain Functional Level page.



3. Click **Raise**, click **OK**, and then click **OK** again.

### Step 4: Install and Configure DHCP

Complete these steps:

1. Install **Dynamic Host Configuration Protocol (DHCP)** as a **Networking Service** component by using **Add or Remove Programs** in the Control Panel.
2. Open the **DHCP** snap-in from the **Administrative Tools** folder (**Start > Programs > Administrative Tools > DHCP**), and then highlight the DHCP server, **DC\_CA.wirelessdemo.local**.
3. Click **Action**, and then click **Authorize** in order to authorize the DHCP service.
4. In the console tree, right-click **DC\_CA.wirelessdemo.local**, and then click **New Scope**.
5. On the Welcome page of the New Scope wizard, click **Next**.
6. On the Scope Name page, type **CorpNet** in the Name field.

**New Scope Wizard**

**Scope Name**  
You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

< Back   Next >   Cancel

7. Click **Next** and fill in these parameters:

- ◆ Start IP address **172.16.100.1**
- ◆ End IP address **172.16.100.254**
- ◆ Length **24**
- ◆ Subnet mask **255.255.255.0**

**New Scope Wizard**

**IP Address Range**  
 You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length:

Subnet mask:

< Back   Next >   Cancel

8. Click **Next** and enter **172.16.100.1** for the Start IP address and **172.16.100.100** for the End IP address to be excluded. Then click **Next**. This reserves the IP addresses in the range from 172.16.100.1 to 172.16.100.100. These reserve IP addresses are not allotted by the DHCP server.

**New Scope Wizard**

**Add Exclusions**  
 Exclusions are addresses or a range of addresses that are not distributed by the server.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:    End IP address:    Add

Excluded address range:

Remove

< Back   Next >   Cancel

9. On the Lease Duration page, click **Next**.

10. On the Configure DHCP Options page, choose **Yes, I want to configure these options now** and click **Next**.

The screenshot shows a window titled "New Scope Wizard" with a blue header bar. Below the header, the title "Configure DHCP Options" is displayed in bold. To the right of the title is a folder icon. The main text reads: "You have to configure the most common DHCP options before clients can use the scope." Below this, a paragraph explains: "When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope." Another paragraph states: "The settings you select here are for this scope and override settings configured in the Server Options folder for this server." A question follows: "Do you want to configure the DHCP options for this scope now?" There are two radio button options: "Yes, I want to configure these options now" (which is selected) and "No, I will configure these options later". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

11. On the Router (Default Gateway) page add the default router address of **172.16.100.1** and click **Next**.

The screenshot shows a window titled "New Scope Wizard" with a blue header bar. Below the header, the title "Router (Default Gateway)" is displayed in bold. To the right of the title is a folder icon. The main text reads: "You can specify the routers, or default gateways, to be distributed by this scope." Below this, a paragraph states: "To add an IP address for a router used by clients, enter the address below." There is a text input field labeled "IP address:" with a dotted cursor. Below the input field is a list box containing the IP address "172.16.100.1". To the right of the list box are four buttons: "Add", "Remove", "Up", and "Down". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

12. On the Domain Name and DNS Servers page, type **wirelessdemo.local** in the Parent domain field, type **172.16.100.26** in the IP address field, and then click **Add** and click **Next**.

**New Scope Wizard**

**Domain Name and DNS Servers**

The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

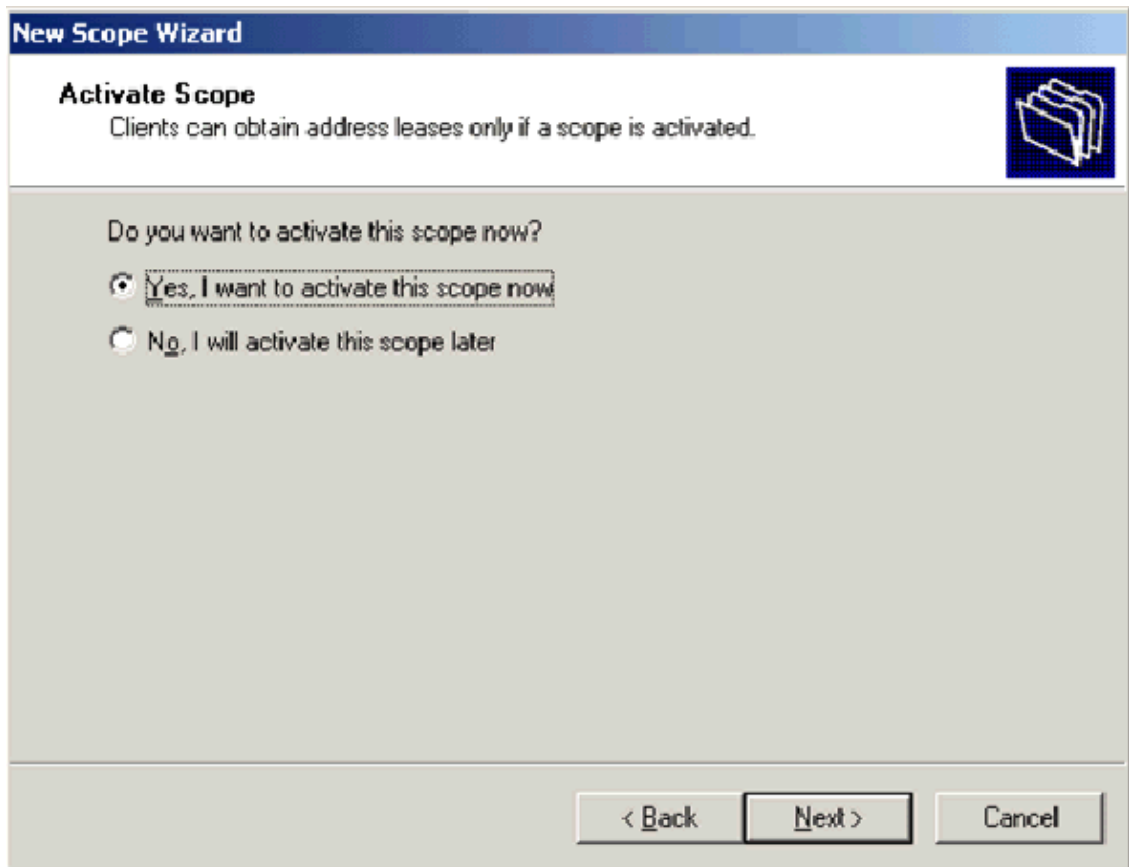
Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:	IP address:
<input type="text"/>	<input type="text" value="172.16.100.26"/>

<

13. On the WINS Servers page, click **Next**.
14. On the Activate Scope page, choose **Yes, I want to activate this scope now** and click **Next**.



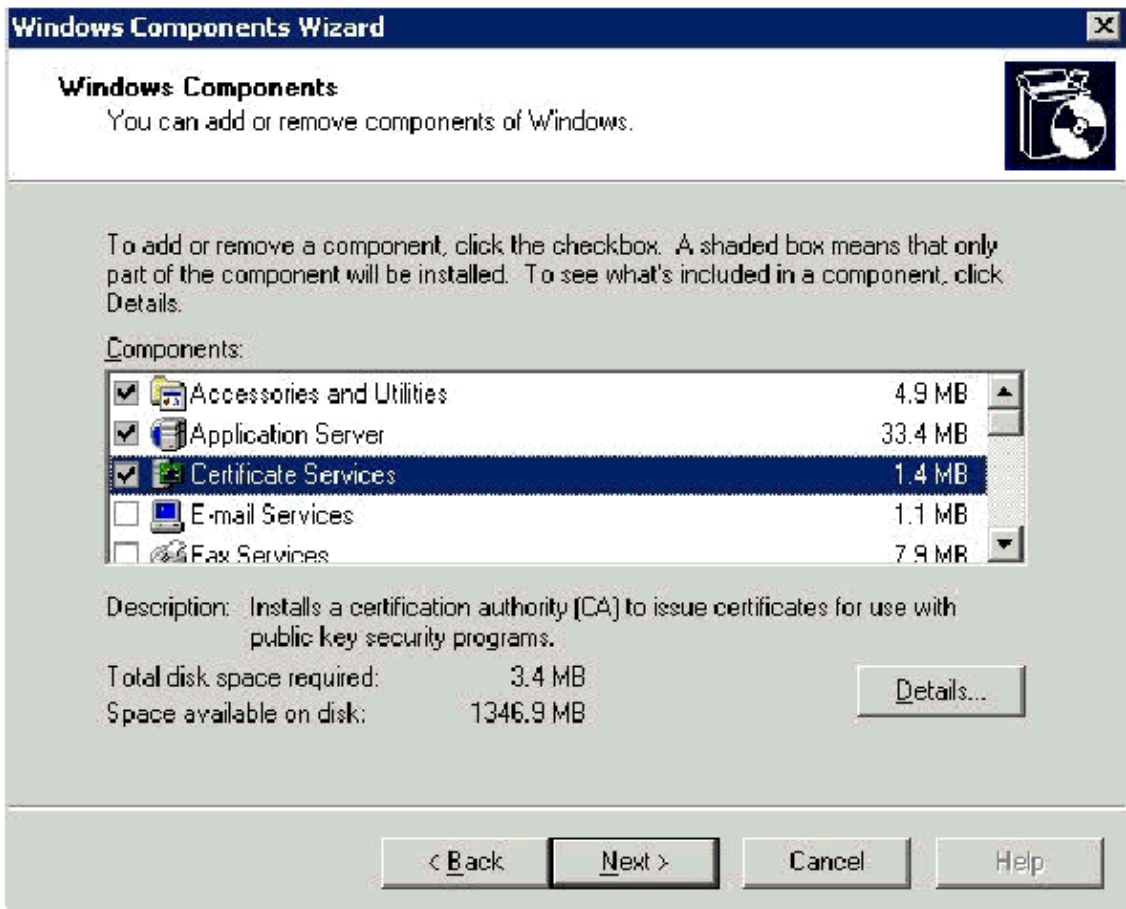
15. When you finish with the New Scope Wizard page, click **Finish**.

### **Step 5: Install Certificate Services**

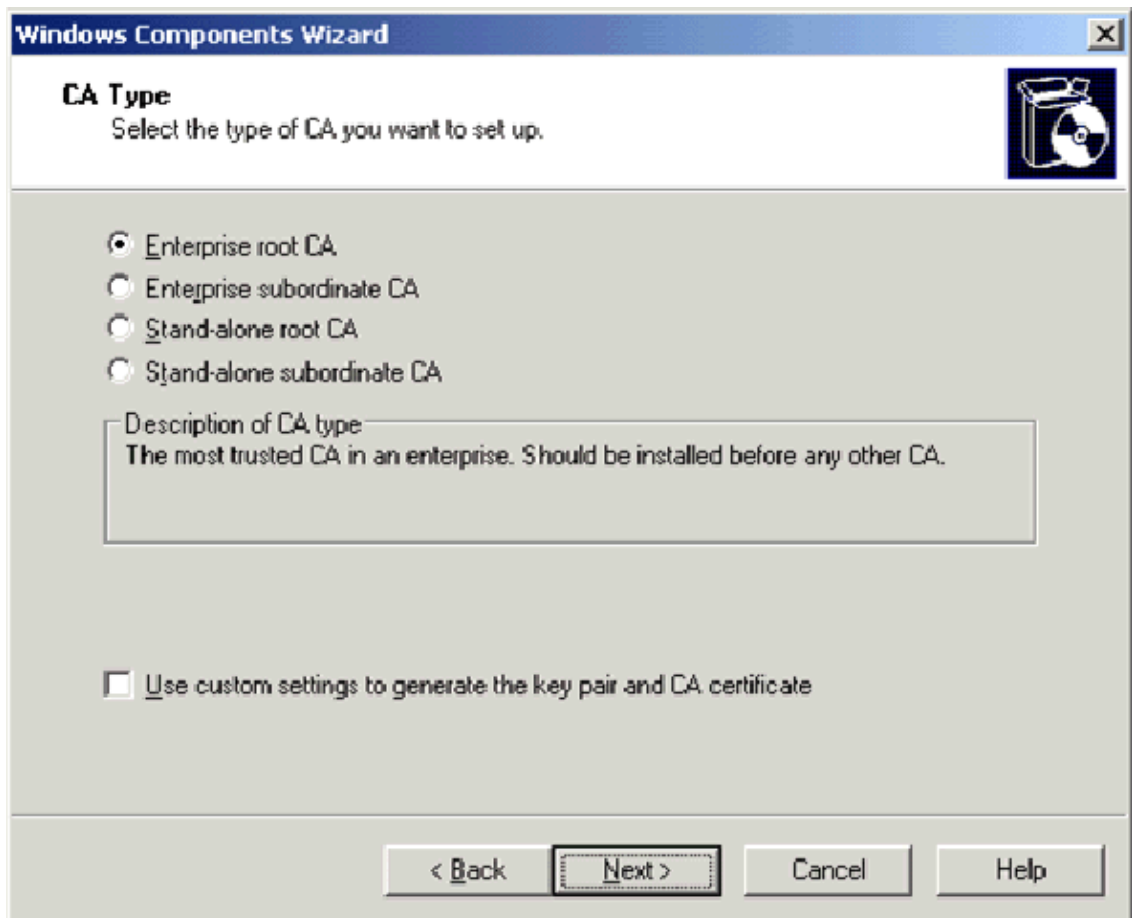
Complete these steps:

**Note:** IIS must be installed before you install Certificate Services and the user should be part of the Enterprise Admin OU.

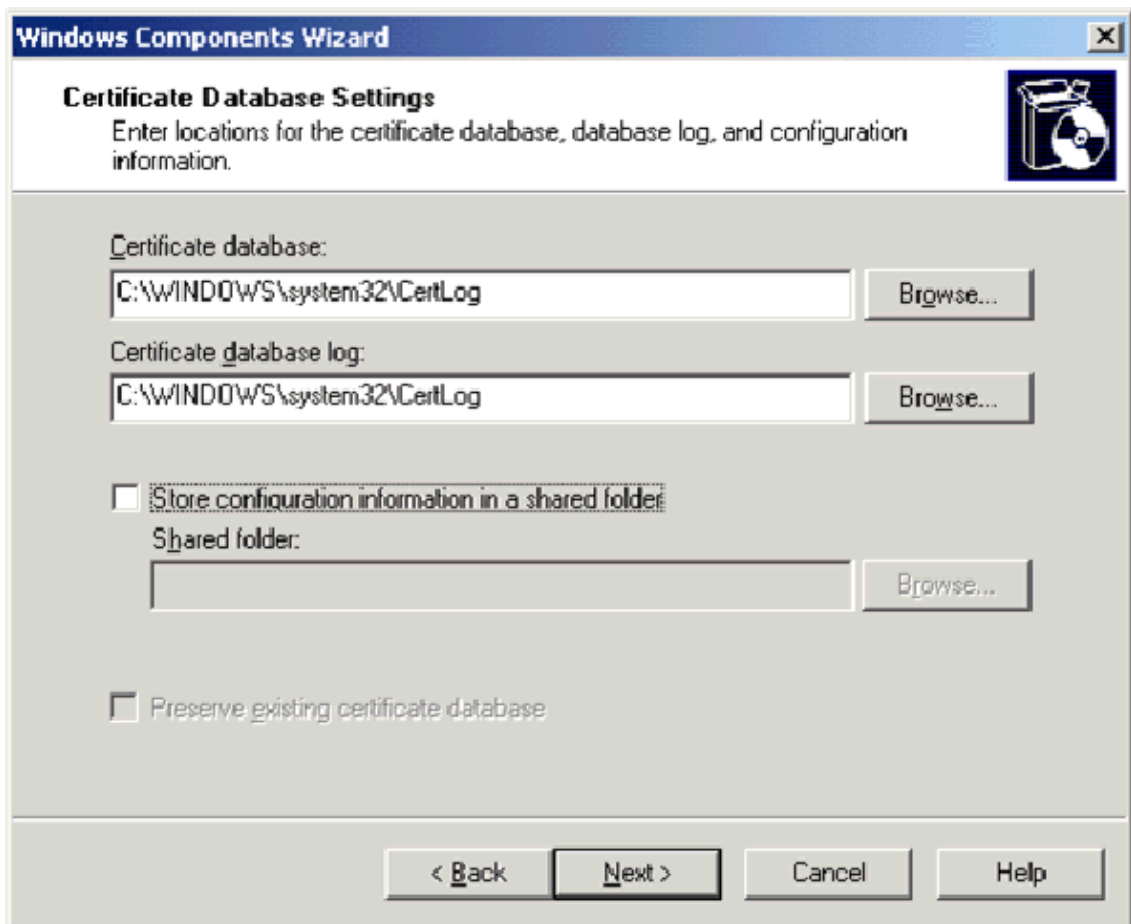
1. In Control Panel, open **Add or Remove Programs**, and then click **Add/Remove Windows Components**.
2. In the Windows Components Wizard page, choose **Certificate Services**, and then click **Next**.



3. On the CA Type page, choose **Enterprise root CA** and click **Next**.



4. In the CA Identifying Information page, type **wirelessdemoca** in the Common name for this CA box. You can also enter the other optional details. Then click **Next** and accept the defaults on the Certificate Database Settings page.



5. Click **Next**. Upon completion of the installation, click **Finish**.
6. Click **OK** after you read the warning message about installing IIS.

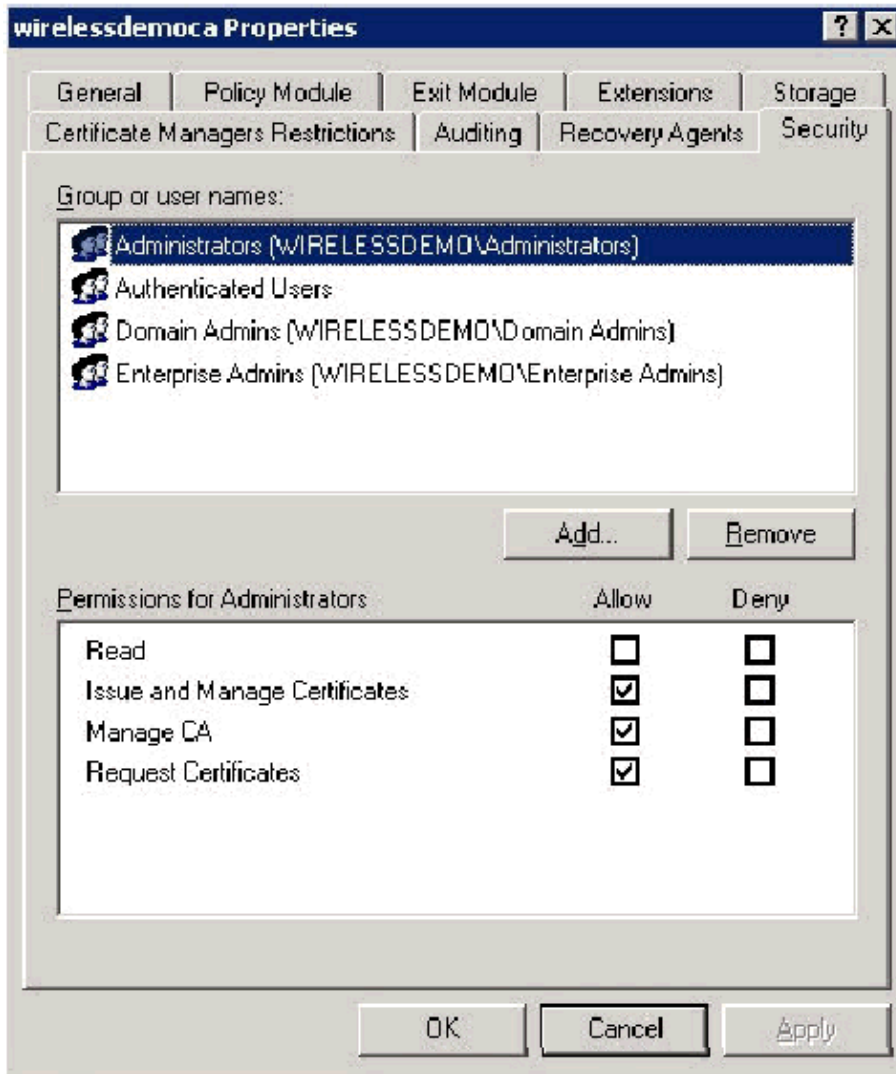
### Step 6: Verify Administrator Permissions for Certificates

Complete these steps:

1. Choose **Start > Administrative Tools > Certification Authority**.
2. Right-click **wirelessdemoca CA** and then click **Properties**.
3. On the Security tab, click **Administrators** in the **Group or User names** list.
4. In the Permissions or Administrators list, verify that these options are set to **Allow**:

- ◆ Issue and Manage Certificates
- ◆ Manage CA
- ◆ Request Certificates

If any of these are set to Deny or are not selected, set the permission to **Allow**.



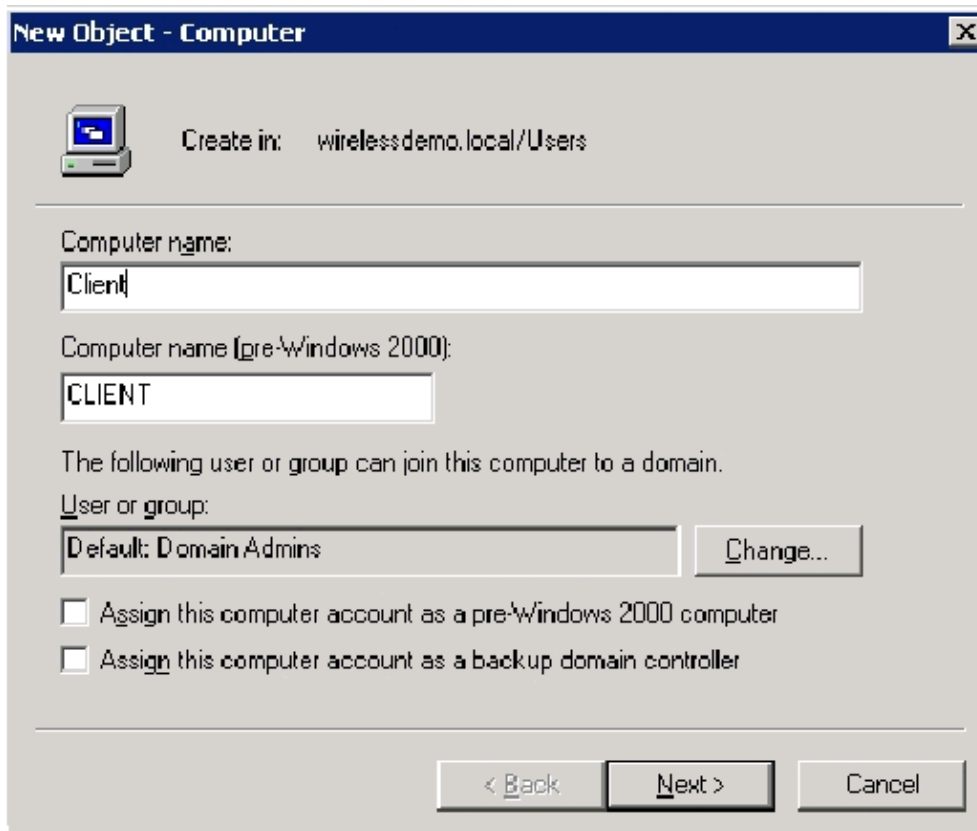
5. Click **OK** to close the wirelessdemoca CA Properties dialog box, and then close Certification Authority.

### Step 7: Add Computers to the Domain

Complete these steps:

**Note:** If the computer is already added to the domain, proceed to Add Users to the Domain.

1. Open the **Active Directory Users and Computers** snap-in.
2. In the console tree, expand **wirelessdemo.local**.
3. Right-click **Users**, click **New**, and then click **Computer**.
4. In the New Object - Computer dialog box, type the name of the computer in the Computer name field and click **Next**. This example uses the computer name **Client**.



5. In the Managed dialog box, click **Next**.
6. In the New Object - Computer dialog box, click **Finish**.
7. Repeat steps 3 through 6 in order to create additional computer accounts.

### Step 8: Allow Wireless Access to Computers

Complete these steps:

1. In the Active Directory Users and Computers console tree, click the **Computers** folder and right-click on the computer for which you want to assign wireless access. This example shows the procedure with computer **Client** which you added in Step 7. Click **Properties**, and then go to the **Dial-in** tab.
2. Choose **Allow access** and click **OK**.

### Step 9: Add Users to the Domain

Complete these steps:

1. In the Active Directory Users and Computers console tree, right-click **Users**, click **New**, and then click **User**.
2. In the New Object - User dialog box, type the name of the Wireless user. This example uses the name **WirelessUser** in the First name field, and **WirelessUser** in the User logon name field. Click **Next**.

**New Object - User**

Create in: wirelessdemo.local/Users

First name: WirelessUser Initials: [ ]

Last name: [ ]

Full name: WirelessUser

User logon name: WirelessUser @wirelessdemo.local

User logon name (pre-Windows 2000): WIRELESSDEMO\ WirelessUser

< Back Next > Cancel

3. In the New Object - User dialog box, type a password of your choice in the Password and Confirm password fields. Clear the **User must change password at next logon** check box, and click **Next**.

**New Object - User**

Create in: wirelessdemo.local/Users

Password: [ ]

Confirm password: [ ]

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

4. In the New Object - User dialog box, click **Finish**.
5. Repeat steps 2 through 4 in order to create additional user accounts.

## Step 10: Allow Wireless Access to Users

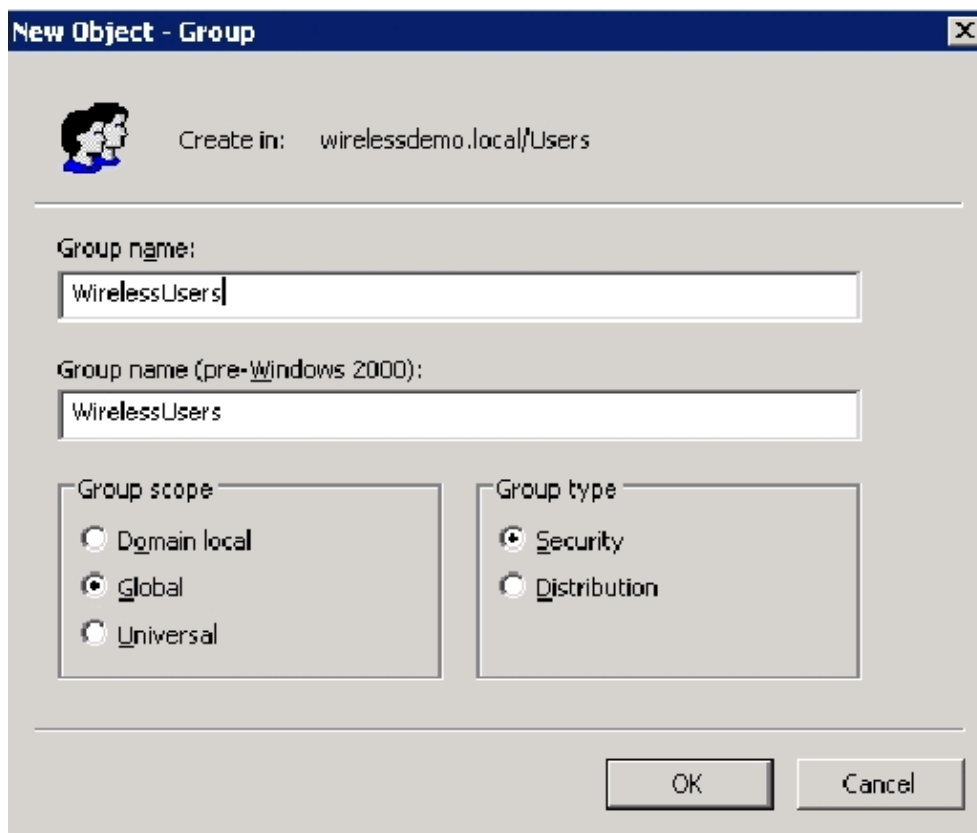
Complete these steps:

1. In the **Active Directory Users and Computers** console tree, click the **Users** folder, right-click **WirelessUser**, click **Properties**, and then go to the Dial-in tab.
2. Choose **Allow access** and click **OK**.

## Step 11: Add Groups to the Domain

Complete these steps:

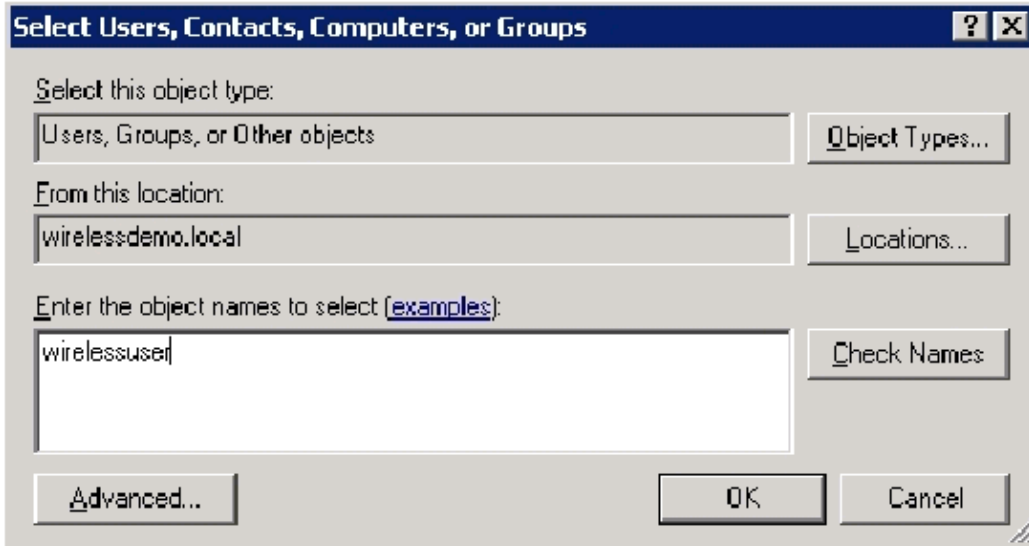
1. In the **Active Directory Users and Computers** console tree, right-click **Users**, click **New**, and then click **Group**.
2. In the New Object Group dialog box, type the name of the group in the Group name field and click **OK**. This document uses the group name **WirelessUsers**.



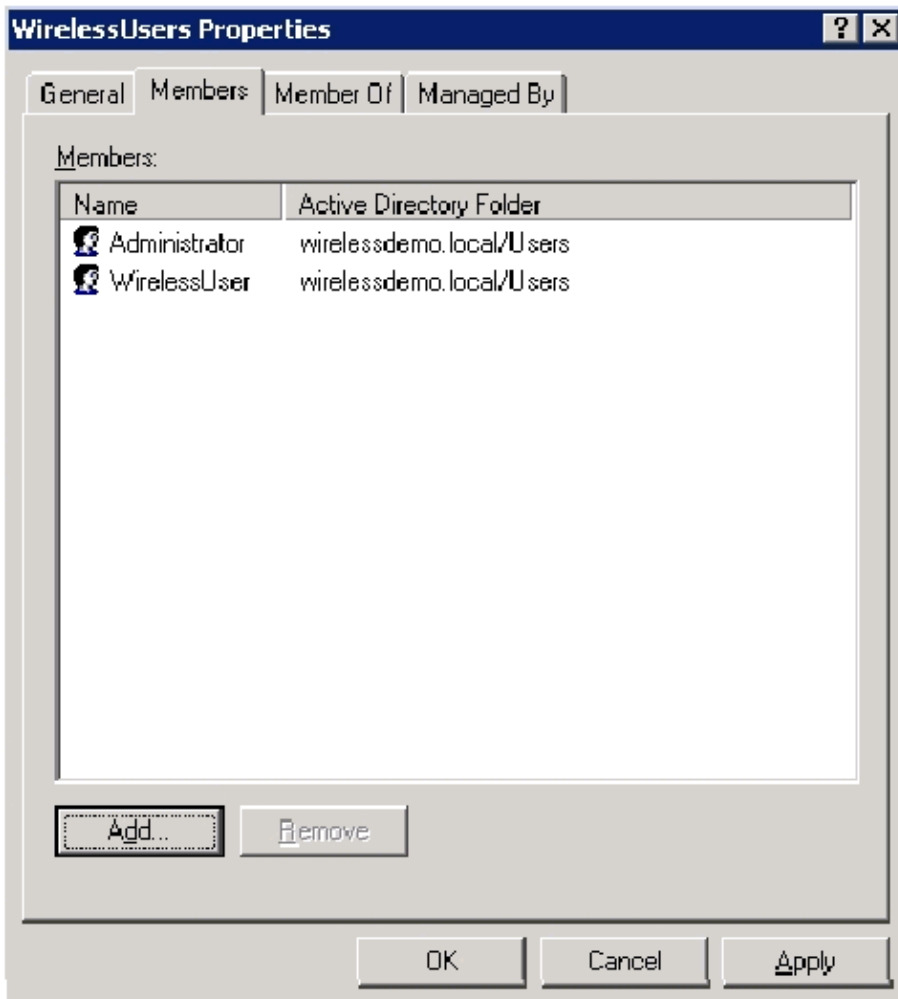
## Step 12: Add Users to the WirelessUsers Group

Complete these steps:

1. In the details pane of Active Directory Users and Computers, double-click on the group **WirelessUsers**.
2. Go to the Members tab and click **Add**.
3. In the Select Users, Contacts, Computers, or Groups dialog box, type the name of the users that you want to add to the group. This example shows how to add the user **wirelessuser** to the group. Click **OK**.



4. In the Multiple Names Found dialog box, click **OK**. The WirelessUser user account is added to the WirelessUsers group.

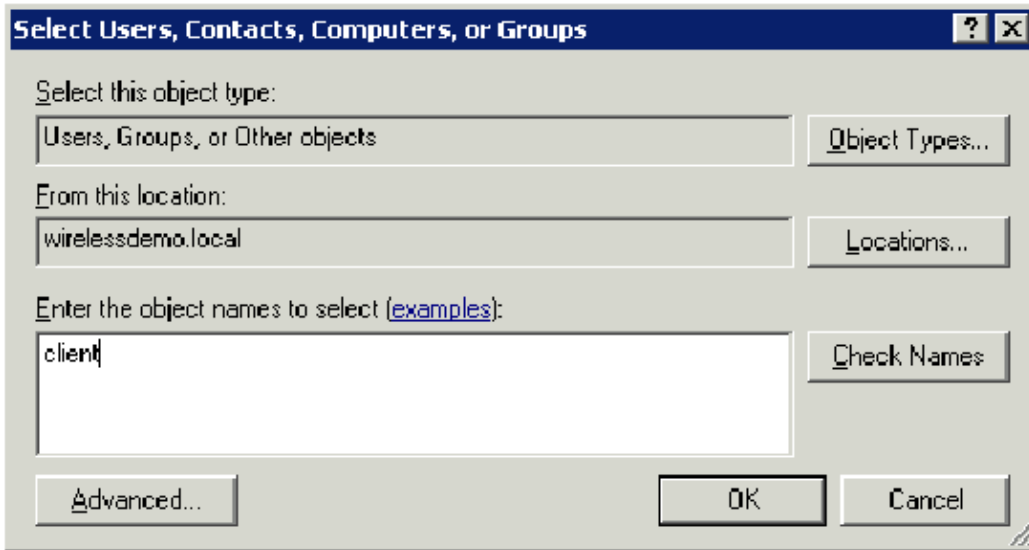


5. Click **OK** in order to save changes to the WirelessUsers group.
6. Repeat this procedure to add more users to the group.

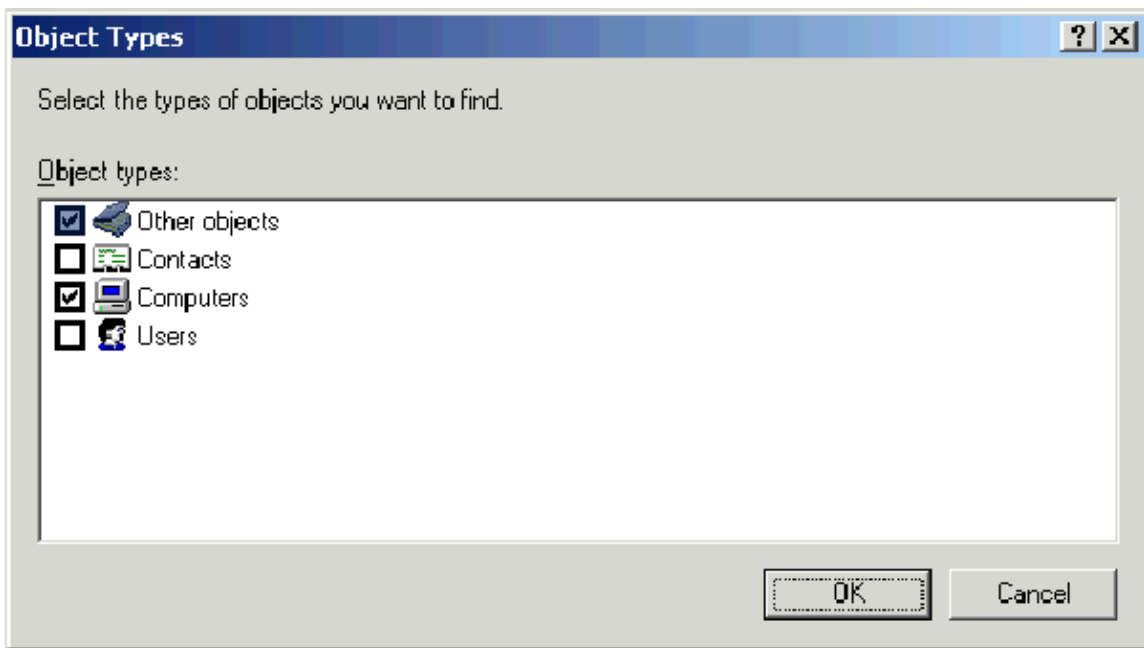
### Step 13: Add Client Computers to the WirelessUsers Group

Complete these steps:

1. Repeat steps 1 and 2 in the Add Users to the WirelessUsers Group section of this document
2. In the Select Users, Contacts, or Computers dialog box, type the name of the computer that you want to add to the group. This example shows how to add the computer named **Client** to the group.



3. Click **Object Types**, clear the **Users** check box, and then check **Computers**.



4. Click **OK** twice. The CLIENT computer account is added to the WirelessUsers group.
5. Repeat the procedure to add more computers to the group.

## Windows Standard 2003 Setup with Cisco Secure ACS 4.0

Cisco Secure ACS is a computer that runs Windows Server 2003 with SP1, Standard Edition, that provides RADIUS authentication and authorization for the controller. Complete the procedures in this section in order to configure ACS as a RADIUS server:

### Basic Installation and Configuration

Complete these steps:

1. Install Windows Server 2003 with SP1, Standard Edition, as a **member server** named **ACS** in the **wirelessdemo.local** domain.

**Note:** The ACS server name appears as `cisco_w2003` in the remaining configurations. Substitute **ACS** or `cisco_w2003` on the remaining lab setup.

2. For the local area connection, configure the TCP/IP protocol with the IP address of **172.16.100.26**, the subnet mask of **255.255.255.0**, and the DNS server IP address of **127.0.0.1**.

## Cisco Secure ACS 4.0 Installation

**Note:** Refer to the Installation Guide for Cisco Secure ACS 4.0 for Windows for more information on how to configure Cisco Secure ACS 4.0 for Windows.

Complete these steps:

1. Use a Domain Administrator account in order to login to the computer named ACS to install Cisco Secure ACS.

**Note:** Only installations performed at the computer where you install Cisco Secure ACS are supported. Remote installations performed using Windows Terminal Services or products such as Virtual Network Computing (VNC) are not tested, and are not supported.

2. Insert the Cisco Secure ACS CD into a CD-ROM drive on the computer.
3. If the CD-ROM drive supports the Windows autorun feature, the Cisco Secure ACS for Windows Server dialog box appears.

**Note:** If the computer does not have a required service pack installed, a dialog box appears. Windows service packs can be applied either before or after you install Cisco Secure ACS. You can continue with the installation, but the required service pack must be applied after the installation is complete. Otherwise, Cisco Secure ACS might not function reliably.

4. Perform one of these tasks:

- ◆ If the Cisco Secure ACS for Windows Server dialog box appears, click **Install**.
- ◆ If the Cisco Secure ACS for Windows Server dialog box does not appear, run **setup.exe**, located in the root directory of the Cisco Secure ACS CD.

5. The Cisco Secure ACS Setup dialog box displays the software license agreement.
6. Read the software license agreement. If you accept the software license agreement, click **Accept**.

The Welcome dialog box displays basic information about the setup program.

7. After you have read the information in the Welcome dialog box, click **Next**.
8. The Before You Begin dialog box lists items that you must complete before you continue with the installation. If you have completed all items listed in the Before You Begin dialog box, check the corresponding box for each item and click **Next**.

**Note:** If you have not completed all items listed in the Before You Begin dialog box, click **Cancel** and then click **Exit Setup**. After you complete all items listed in the Before You Begin dialog box, restart the installation.

9. The Choose Destination Location dialog box appears. Under Destination Folder, the installation location appears. This is the drive and path where the setup program installs Cisco Secure ACS.
10. If you want to change the installation location, complete these steps:
  - a. Click **Browse**. The Choose Folder dialog box appears. The Path box contains the installation location.
  - b. Change the installation location. You can either type the new location in the Path box or use the Drives and Directories lists to select a new drive and directory. The installation location

must be on a drive local to the computer.

**Note:** Do not specify a path that contains a percent character, "%". If you do so, the installation might appear to continue properly but fails before it completes.

c. Click **OK**.

**Note:** If you specified a folder that does not exist, the setup program displays a dialog box to confirm the creation of the folder. In order to continue, click **Yes**.

11. In the Choose Destination Location dialog box, the new installation location appears under Destination Folder.
12. Click **Next**.
13. The Authentication Database Configuration dialog box lists options for authenticating users. You can authenticate with the Cisco Secure user database only, or also with a Windows user database.

**Note:** After you install Cisco Secure ACS, you can configure authentication support for all external user database types in addition to Windows user databases.

14. If you want to authenticate users with the Cisco Secure user database only, choose the **Check the Cisco Secure ACS database only** option.
15. If you want to authenticate users with a Windows Security Access Manager (SAM) user database or Active Directory user database in addition to the Cisco Secure user database, complete these steps:
  - a. Choose the **Also check the Windows User Database** option.
  - b. The **Yes, refer to "Grant dialin permission to user" setting** check-box becomes available.

**Note:** The **Yes, refer to "Grant dialin permission to user" setting** check-box applies to all forms of access controlled by Cisco Secure ACS, not just dial-in access. For example, a user who accesses the network through a VPN tunnel does not dial into a network access server. However, if the **Yes, refer to "Grant dialin permission to user" setting** box is checked, Cisco Secure ACS applies the Windows user dial-in permissions in order to determine whether to grant the user access to the network.

- c. If you want to allow access to users who are authenticated by a Windows domain user database only when they have dial-in permission in their Windows account, check the **Yes, refer to "Grant dialin permission to user" setting** box.
16. Click **Next**.
  17. The setup program installs Cisco Secure ACS and updates the Windows registry.
  18. The Advance Options dialog box lists several features of Cisco Secure ACS that are not enabled by default. For more information about these features, refer to the User Guide for Cisco Secure ACS for Windows Server, version 4.0.

**Note:** The listed features appear in the Cisco Secure ACS HTML interface only if you enable them. After installation, you can enable or disable them on the Advanced Options page in the Interface Configuration section.

19. For each feature you want to enable, check the corresponding box.
20. Click **Next**.
21. The Active Service Monitoring dialog box appears.

**Note:** After installation, you can configure active service monitoring features on the Active Service Management page in the System Configuration section.

22. If you want Cisco Secure ACS to monitor user authentication services, check the **Enable Login Monitoring** box. From the Script to Execute list, choose the option you want applied in the event of authentication service failure:

◆ **No Remedial Action** Cisco Secure ACS does not run a script.

**Note:** This option is useful if you enable event mail notifications.

- ◆ **Reboot** Cisco Secure ACS runs a script that reboots the computer that runs Cisco Secure ACS.
  - ◆ **Restart All** Cisco Secure ACS restarts all Cisco Secure ACS services.
  - ◆ **Restart RADIUS/TACACS+** Cisco Secure ACS restarts only the RADIUS and TACACS+ services.
23. If you want Cisco Secure ACS to send an e-mail message when service monitoring detects an event, check the **Mail Notification** box.
  24. Click **Next**.
  25. The Database Encryption Password dialog box appears.

**Note:** The Database Encryption Password is encrypted and stored in the ACS registry. You might need to reuse this password when critical problems arise and the database needs to be accessed manually. Keep this password at hand so that Technical Support can gain access to the database. The password can be changed each expiration period.

26. Enter a password for database encryption. The password needs to be at least eight characters long and needs to contain both characters and digits. There are no invalid characters.
27. Click **Next**.
28. The setup program finishes and the Cisco Secure ACS Service Initiation dialog box appears.
29. For each Cisco Secure ACS Services Initiation option you want, check the corresponding box. The actions associated with the options occur after the setup program finishes.

- ◆ **Yes, I want to start the Cisco Secure ACS Service now** Starts the Windows services that compose Cisco Secure ACS. If you do not select this option, the Cisco Secure ACS HTML interface is not available unless you reboot the computer or start the CSAdmin service.
  - ◆ **Yes, I want Setup to launch the Cisco Secure ACS Administrator from my browser following installation** Opens the Cisco Secure ACS HTML interface in the default web browser for the current Windows user account.
  - ◆ **Yes, I want to view the Readme File** Opens the README.TXT file in Windows Notepad.
30. Click **Next**.
  31. If you selected an option, the Cisco Secure ACS services start. The Setup Complete dialog box displays information about the Cisco Secure ACS HTML interface.
  32. Click **Finish**.

**Note:** The rest of the configuration is documented under the section for the EAP type that is configured.

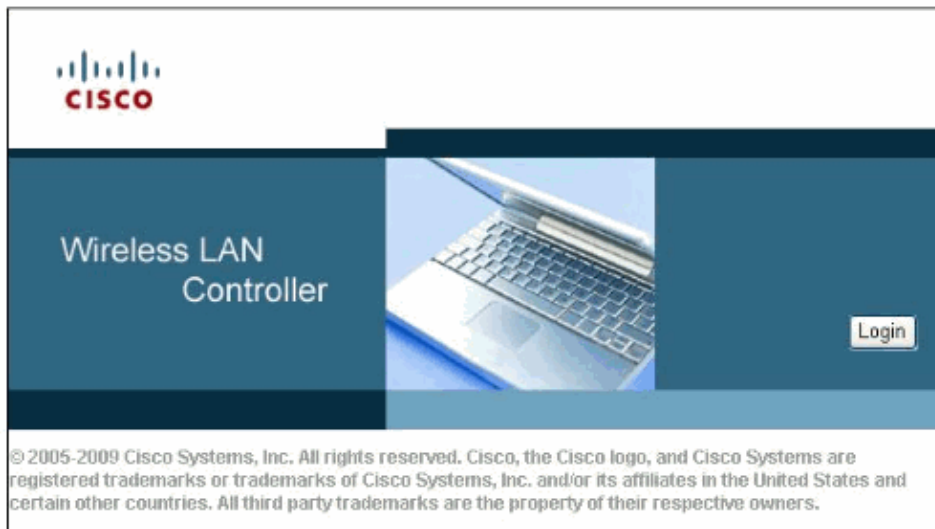
## Cisco LWAPP Controller Configuration

### Create the Necessary Configuration for WPAv2/WPA

Complete these steps:

**Note:** The assumption is that the controller has basic connectivity to the network and IP reachability to the management interface is successful.

1. Browse to **https://172.16.101.252** in order to login to the controller.



2. Click **Login**
3. Login with the default user **admin** and default password **admin**.
4. Create a new Interface for VLAN mapping under **Controller** menu.
5. Click **Interfaces**.
6. Click **New**.
7. In the Interface name field type **Employee**. (This field can be any value you like.)
8. In the VLAN ID field type **20**. (This field can be any VLAN that is carried in the network.)
9. Click **Apply**.
10. Configure the information as this Interfaces > Edit window shows.

The screenshot shows the Cisco Controller configuration page for an interface named 'employee'. The page is divided into several sections:

- General Information:** Interface Name: employee, MAC Address: 09:0b:85:48:53:c0
- Configuration:** Guest Lan: , Quarantine: , Quarantine Vlan Id: 0
- Physical Information:** Port Number: 1, Backup Port: 0, Active Port: 0, Enable Dynamic AP Management:
- Interface Address:** VLAN Identifier: 20, IP Address: 172.16.100.4, Netmask: 255.255.255.0, Gateway: 172.16.100.1
- DHCP Information:** Primary DHCP Server: 172.16.100.25, Secondary DHCP Server: 0.0.0.0

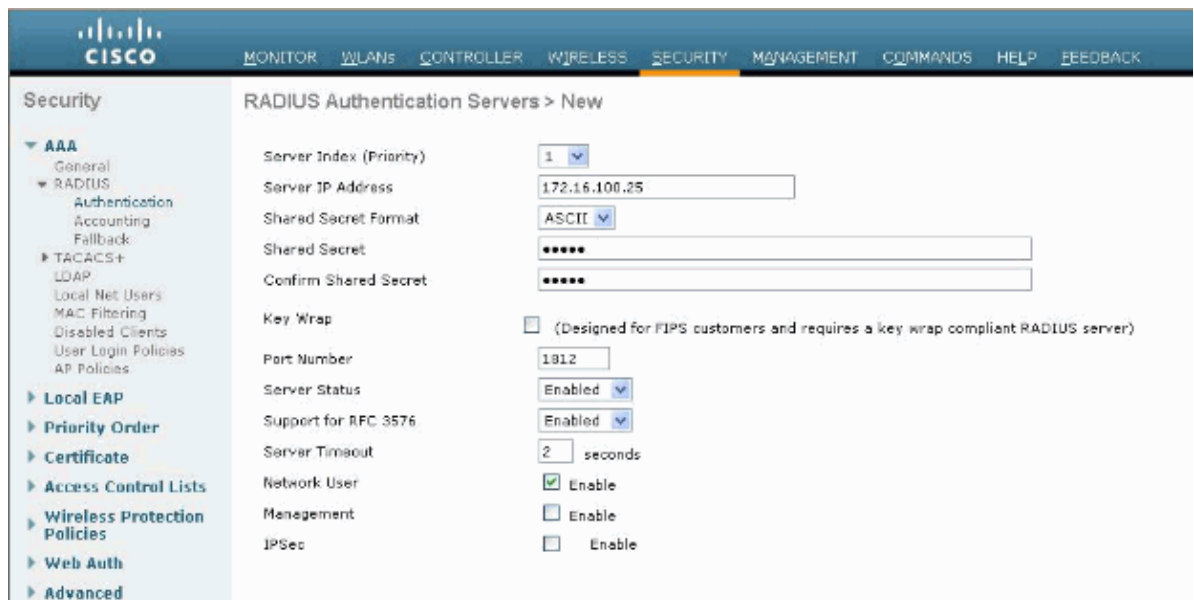
11. Click **Apply**.
12. Click the **WLANS** tab.
13. Choose **Create New** and click **Go**.
14. Enter a Profile Name and in the WLAN SSID field type **Employee**.
15. Choose an ID for the WLAN and click **Apply**.
16. Configure the information for this WLAN when the **WLANS > Edit** window shows.

**Note:** WPAv2 is the chosen Layer 2 encryption method for this lab. In order to allow WPA with TKIP–MIC clients to associate to this SSID, you can also check the **WPA compatibility mode** and **Allow WPA2 TKIP Clients** boxes or those clients that do not support the 802.11i AES encryption method.

The screenshot shows the Cisco Controller configuration page for a WLAN named 'employee'. The page is divided into several sections:

- General:** Profile Name: employee, Type: WLAN, SSID: Employee, Status:  Enabled
- Security Policies:** [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
- Radio Policy:** All
- Interface:** employee
- Broadcast SSID:**  Enabled

17. On the WLANs > Edit screen, click the **General** tab.
18. Ensure that the Status box is checked for **Enabled** and the appropriate **Interface** (employee) is chosen. Also, make sure to check the Enabled check box for Broadcast SSID.
19. Click the **Security** tab.
20. Under the **Layer 2** sub–menu check **WPA + WPA2** for Layer 2 Security. For WPA2 encryption check **AES + TKIP** in order to allow TKIP clients.
21. Choose **802.1x** as the authentication method.
22. Skip the Layer 3 sub–menu as it is not required. Once the RADIUS server is configured the appropriate server can be chosen from the Authentication menu.
23. The **QoS** and **Advanced** tabs can be left at default unless any special configurations are required.
24. Click the **Security** menu to add the RADIUS Server.
25. Under the **RADIUS** sub–menu click **Authentication**. Then, click **New**.
26. Add the RADIUS server IP address (172.16.100.25) which is the ACS server configured earlier.
27. Ensure that the shared key matches the AAA client configured in the ACS server. Ensure that the Network User box is checked and click **Apply**.



28. The basic configuration is now complete and you can begin to test PEAP.

## PEAP Authentication

PEAP with MS–CHAP version 2 requires certificates on the ACS servers but not on the wireless clients. Auto enrollment of computer certificates for the ACS servers can be used to simplify a deployment.

In order to configure DC\_CA to provide autoenrollment for computer and user certificates, complete the procedures in this section.

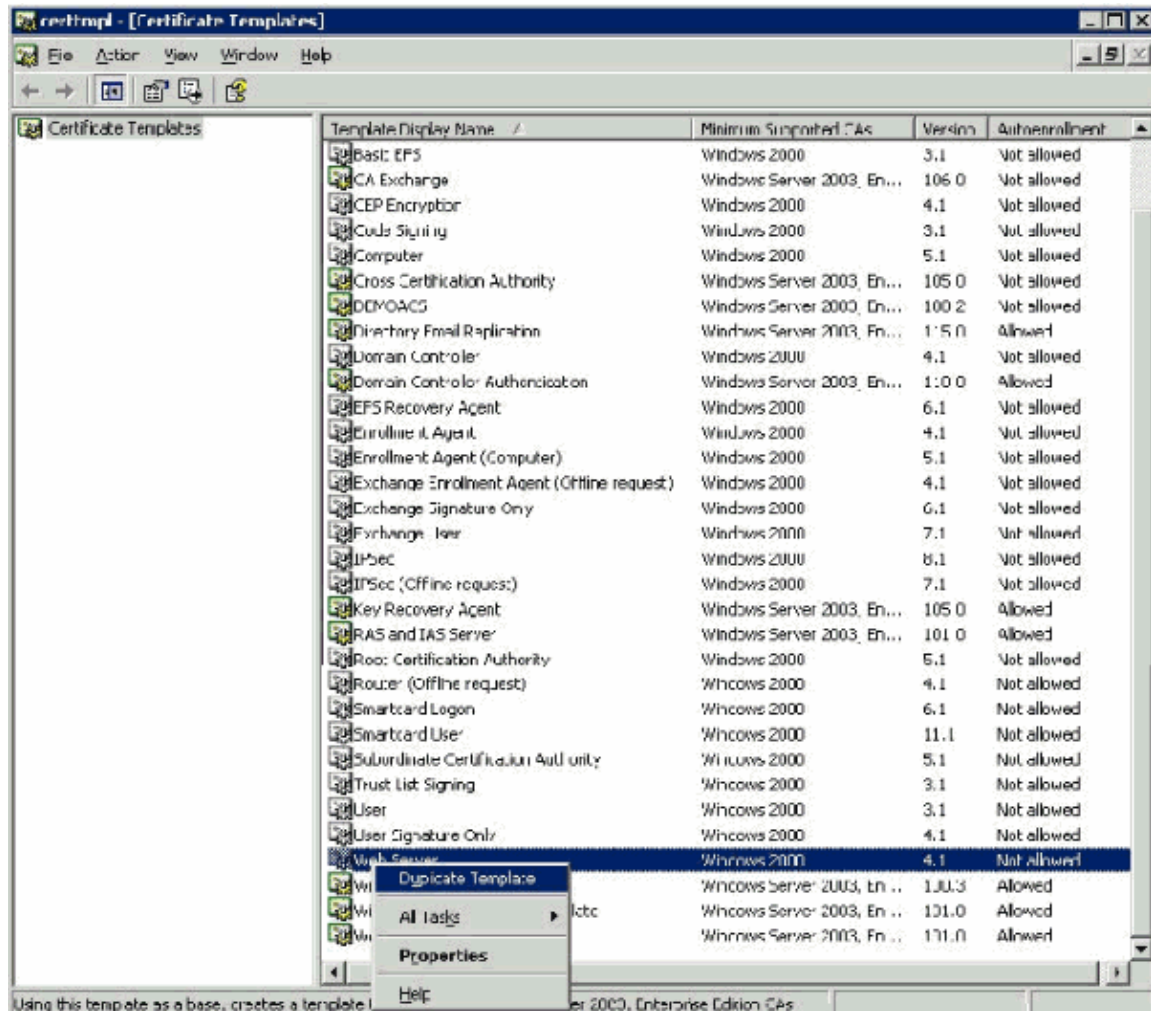
**Note:** Microsoft has changed the Web Server template with the release of the Windows 2003 Enterprise CA so that keys are no longer exportable and the option is greyed out. There are no other certificate templates supplied with certificate services that are for server authentication and give the ability to mark keys as exportable that are available in the drop–down so you have to create a new template that does so.

**Note:** Windows 2000 allows for exportable keys and these procedures do not need to be followed if you use Windows 2000.

## Install the Certificate Templates Snap-in

Complete these steps:

1. Choose **Start > Run**, type **mmc**, and click **OK**.
2. On the File menu, click **Add/Remove Snap-in** and then click **Add**.
3. Under Snap-in, double-click **Certificate Templates**, click **Close**, and then click **OK**.
4. In the console tree, click **Certificate Templates**. All of the certificate templates appear in the Details pane.
5. In order to bypass steps 2 through 4, type **certtmpl.msc** which opens the Certificate Templates snap-in.



## Create the Certificate Template for the ACS Web Server

Complete these steps:

1. In the Details pane of the Certificate Templates snap-in, click the **Web Server** template.
2. On the Action menu, click **Duplicate Template**.

**Properties of New Template** [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | Subject Name

Template display name:  
Copy of Web Server

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name:  
Copy of Web Server

Validity period: 2 years  
Renewal period: 6 weeks

Publish certificate in Active Directory  
 Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply

3. In the Template display name field, type ACS.

**Properties of New Template** [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | **Request Handling** | Subject Name

Template display name:  
ACS

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

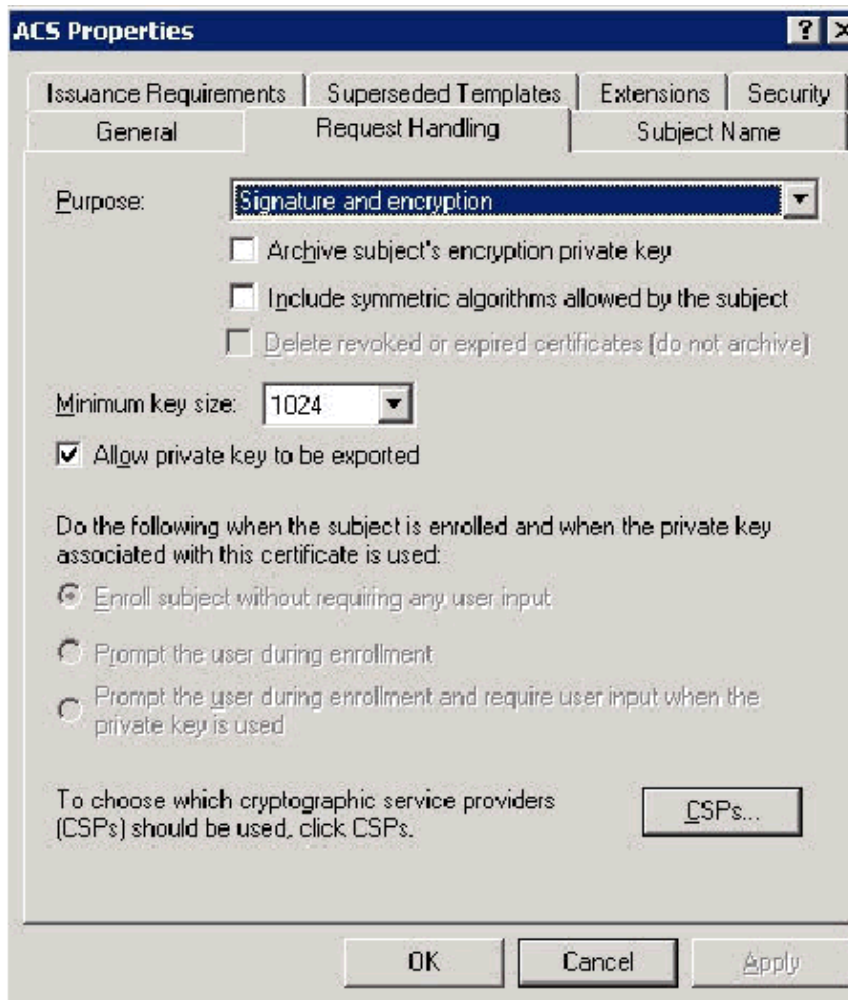
Template name:  
ACS

Validity period: 2 years  
Renewal period: 6 weeks

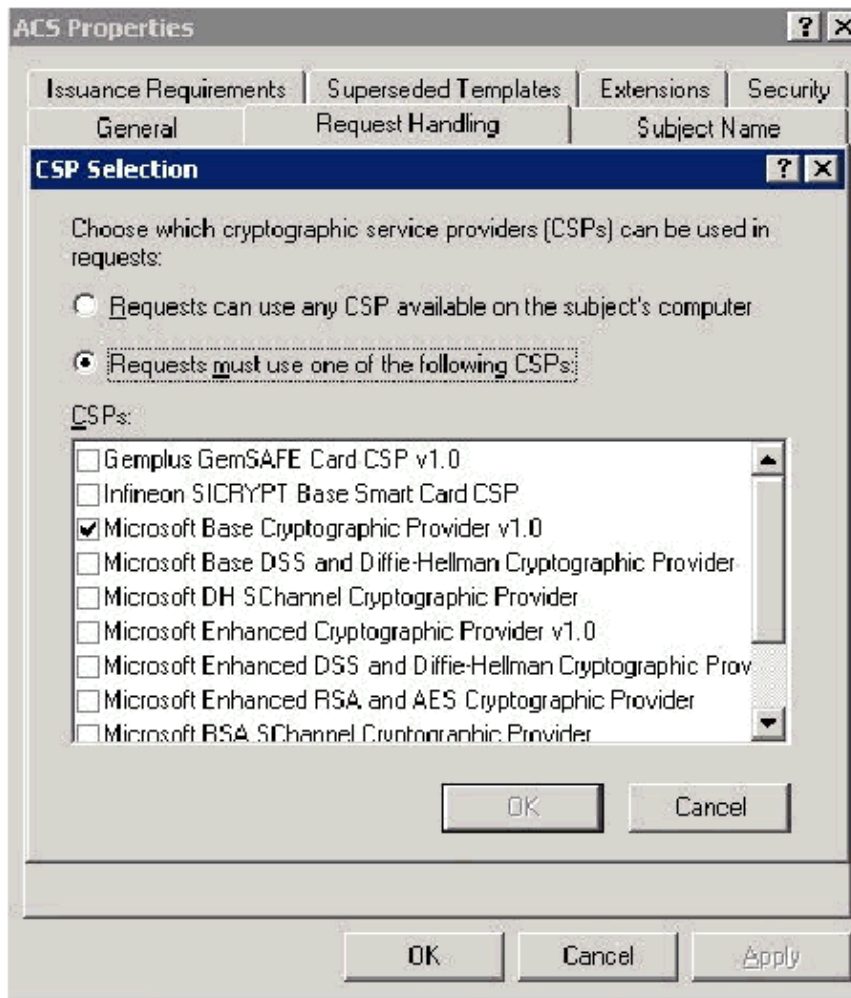
Publish certificate in Active Directory  
 Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply

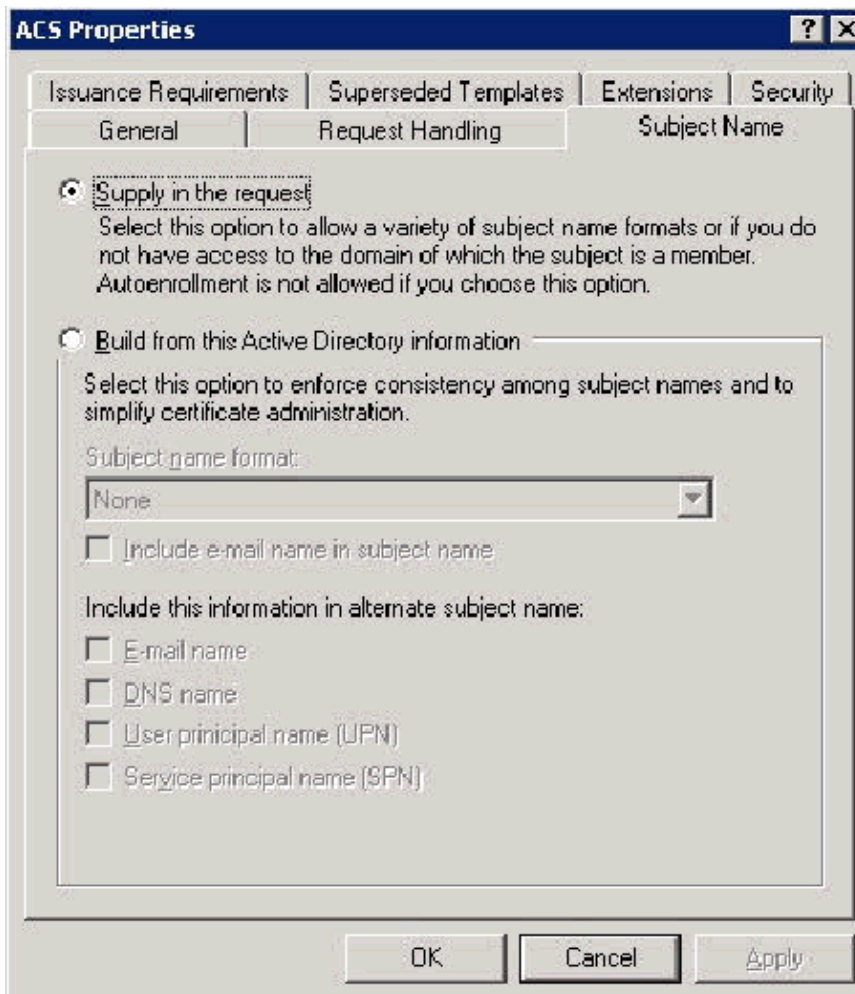
4. Go to the Request Handling tab and check **Allow private key to be exported**. Also ensure that **Signature and Encryption** is selected from the Purpose drop-down menu.



5. Choose **Requests must use one of the following CSPs** and check **Microsoft Base Cryptographic Provider v1.0**. Uncheck any other CSPs that are checked and then click **OK**.

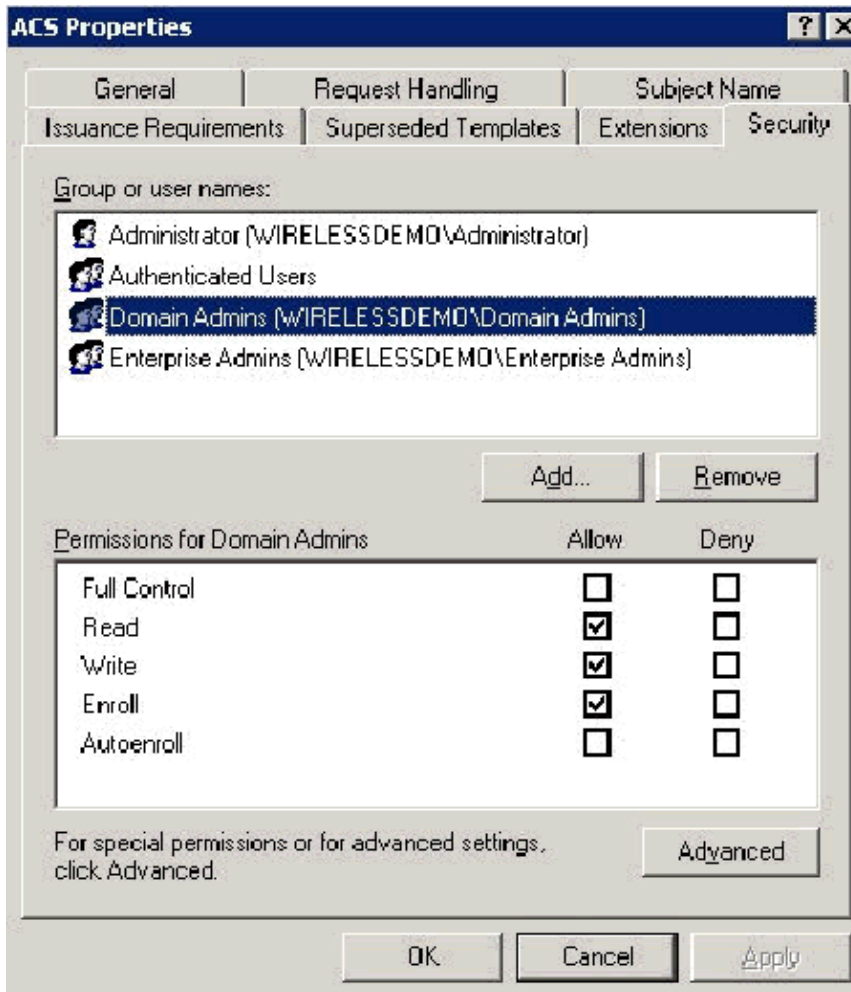


6. Go to the Subject Name tab, choose **Supply in the request** and click **OK**.

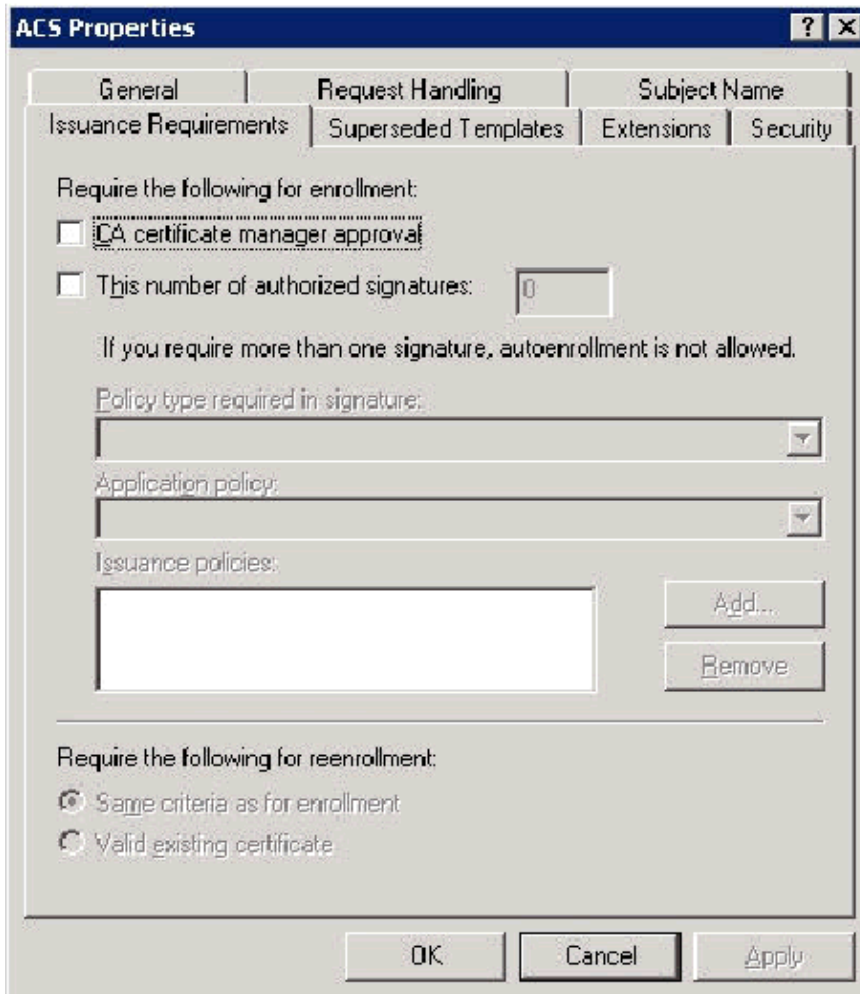


7. Go to the Security tab, highlight the **Domain Admins Group** and ensure that the **Enroll** option is checked under Allowed.

**Important:** If you choose to build from this Active Directory information only check the **User principal name (UPN)** and uncheck the **Include email name** in subject name and E-mail name because an e-mail name was not entered for the Wireless User account in the Active Directory Users and Computers snap-in. If you do not disable these two options, autoenrollment attempts to use e-mail, which results in an autoenrollment error.



8. There are additional security measures if needed to prevent certificates from being automatically pushed out. These can be found under the Issuance Requirements tab. This is not discussed further in this document.

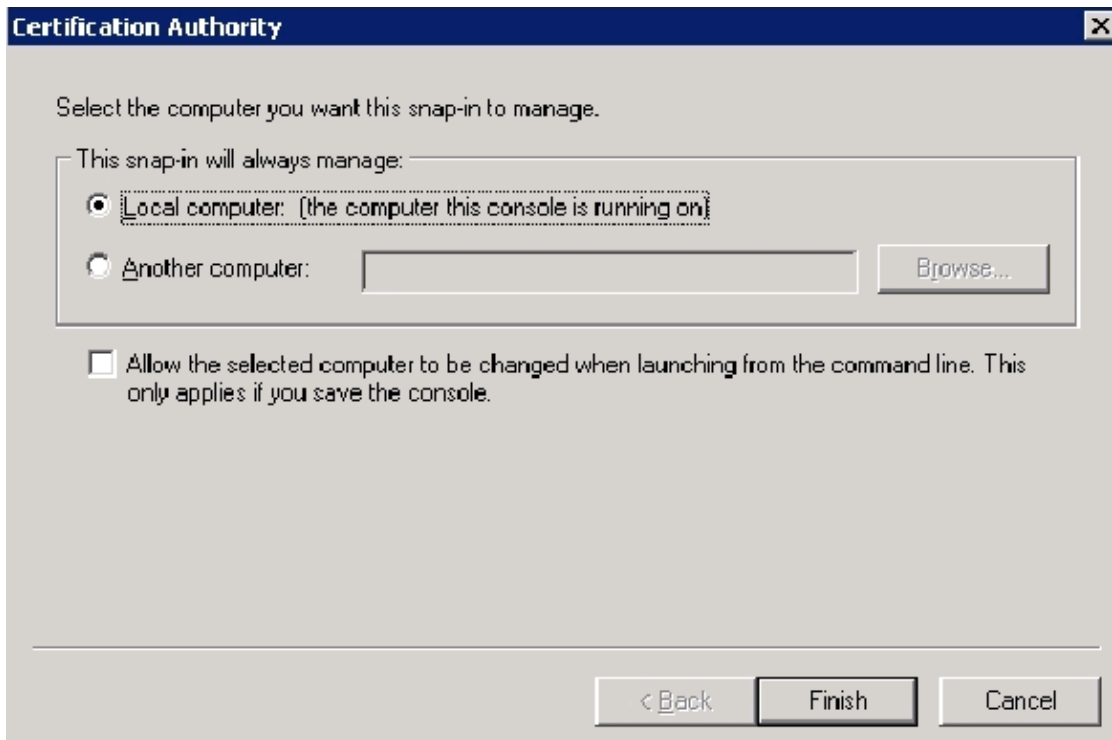


9. Click **OK** to save the template and move onto issuing this template from the Certificate Authority snap-in.

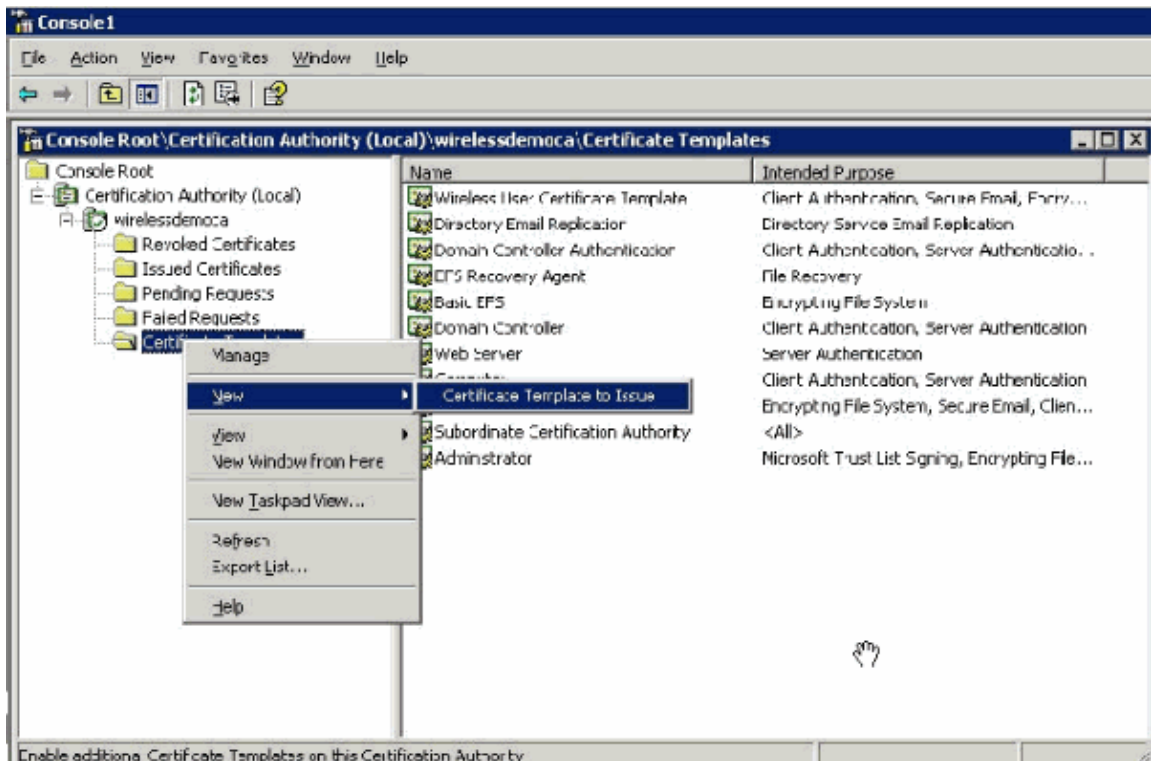
## Enable the New ACS Web Server Certificate Template

Complete these steps:

1. Open the Certification Authority snap-in. Follow steps 1–3 in the Create the Certificate Template for the ACS Web Server section, choose the **Certificate Authority** option, choose **Local Computer** and click **Finish**.

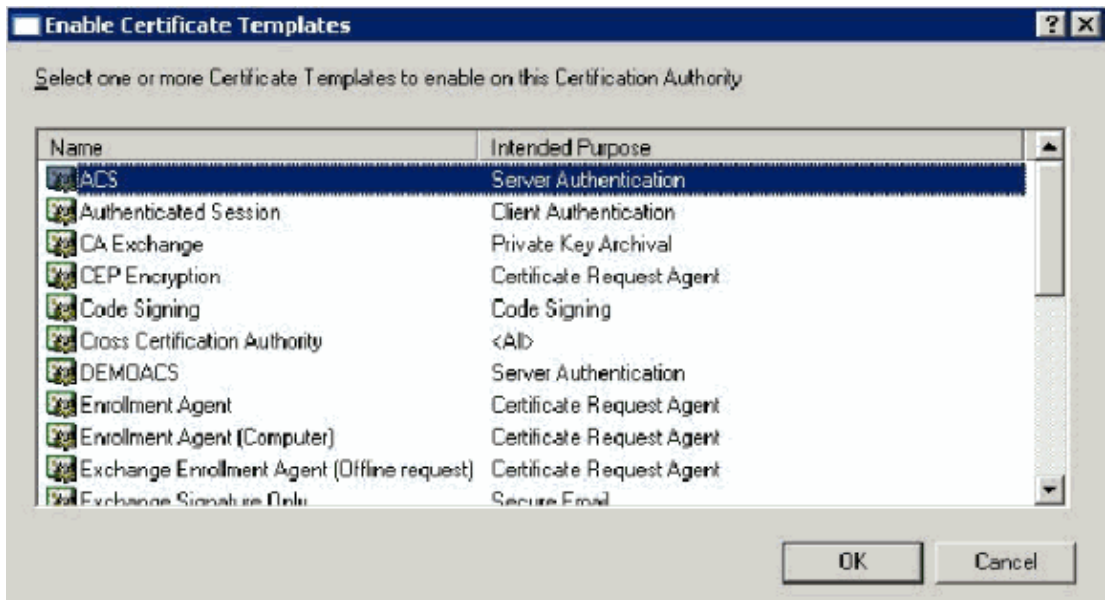


2. In the console tree, expand **wirelessdemoca**, and then right-click **Certificate Templates**.

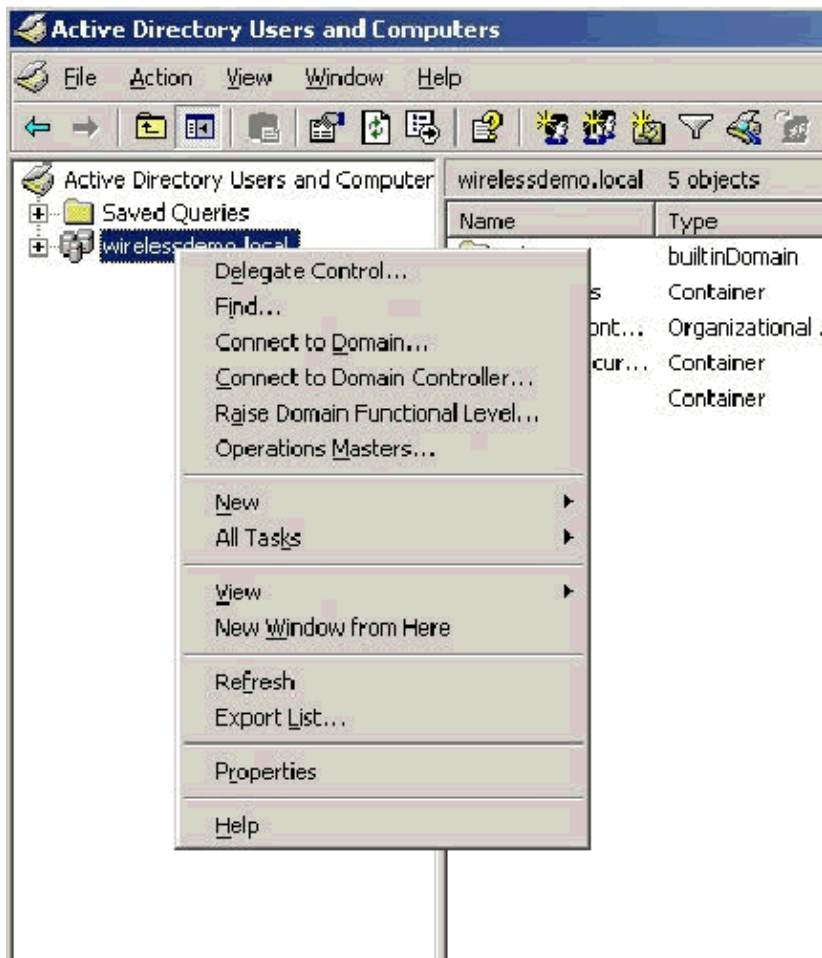


3. Choose **New > Certificate Template to Issue**.

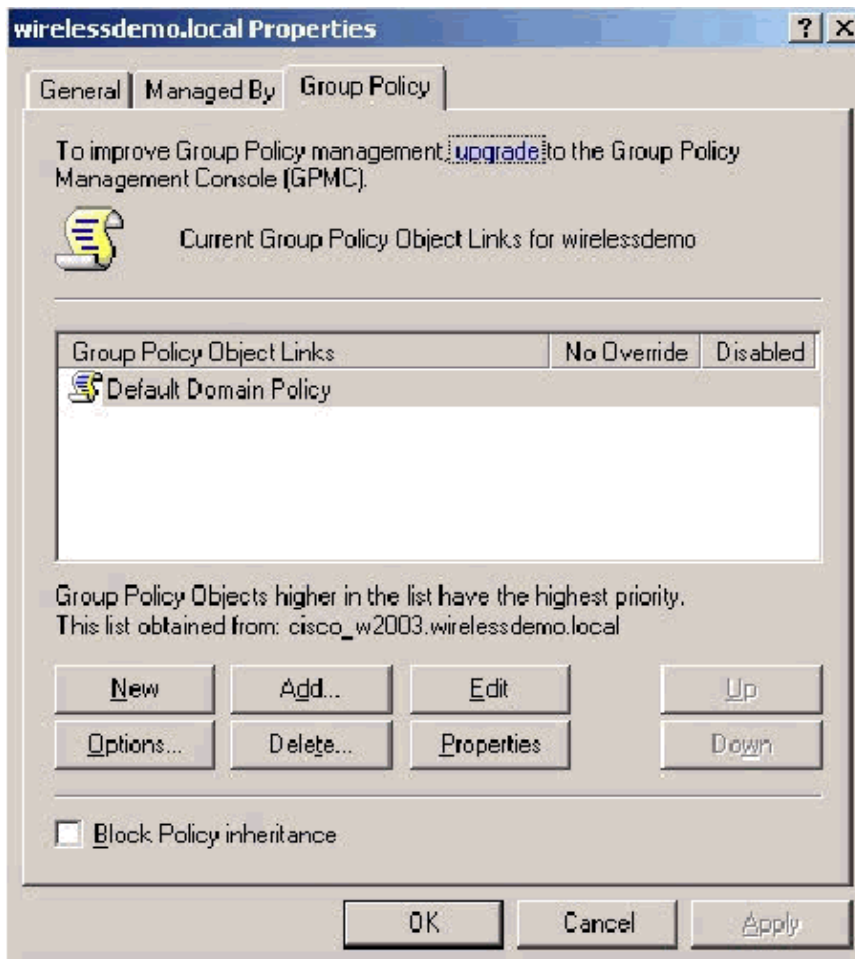
4. Click the ACS Certificate Template.



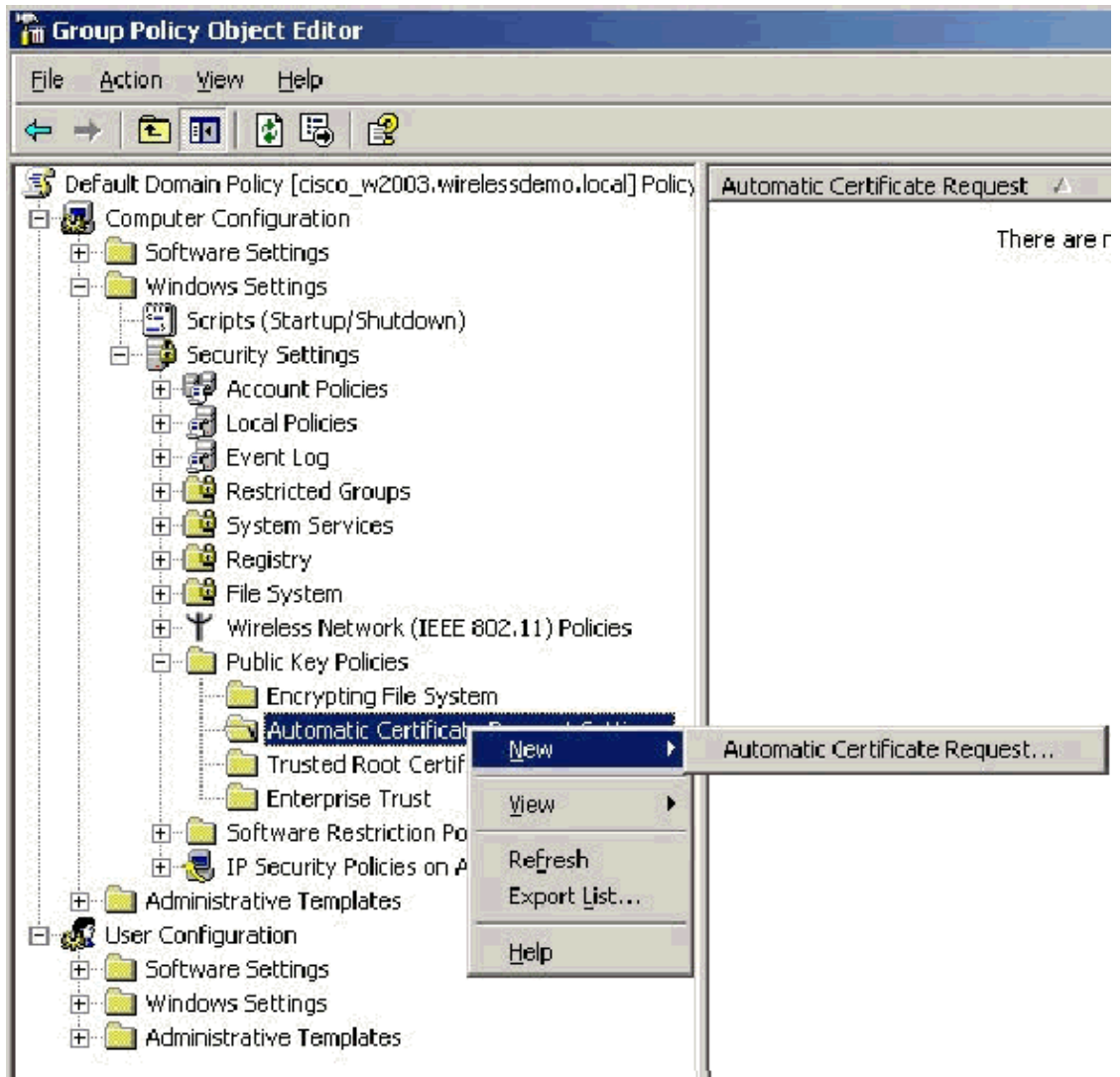
5. Click **OK** and open the **Active Directory Users and Computers** snap-in.
6. In the console tree, double-click **Active Directory Users and Computers**, right-click **wirelessdemo.local**, and then click **Properties**.



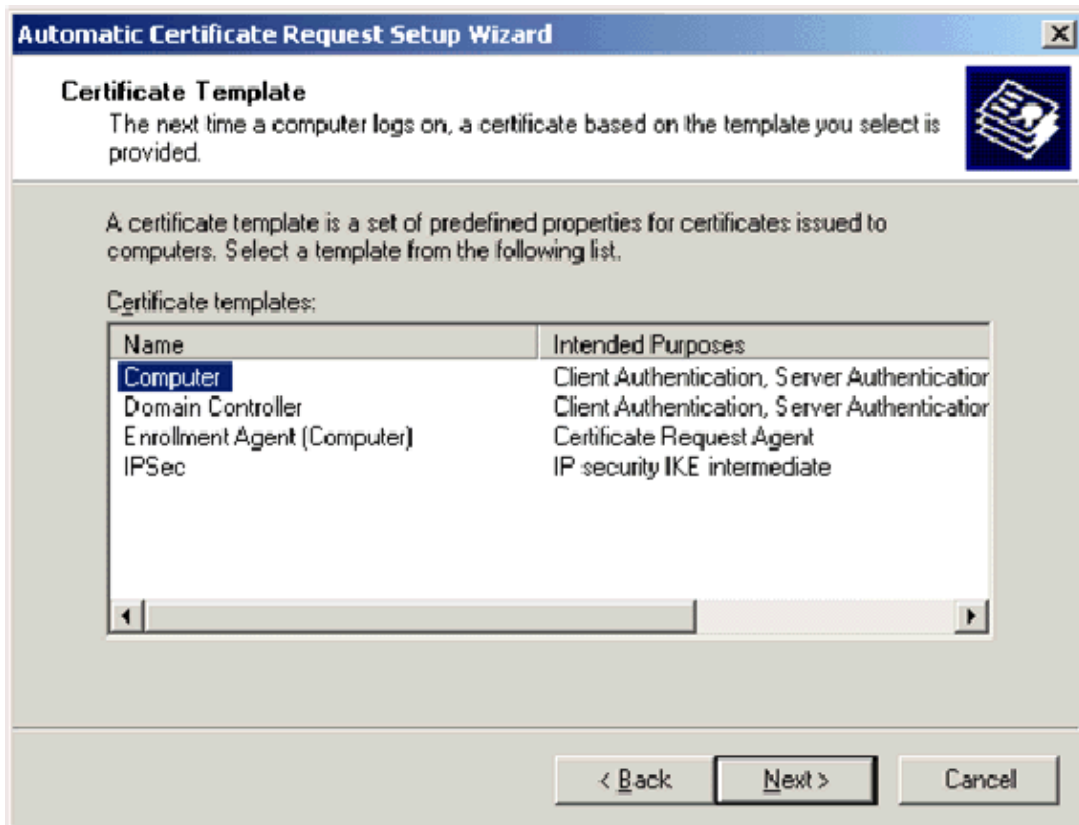
7. On the Group Policy tab, click **Default Domain Policy**, and then click **Edit**. This opens the Group Policy Object Editor snap-in.



8. In the console tree, expand **Computer Configuration > Windows Settings > Security Settings > Public Key Policies**, and then select **Automatic Certificate Request Settings**.

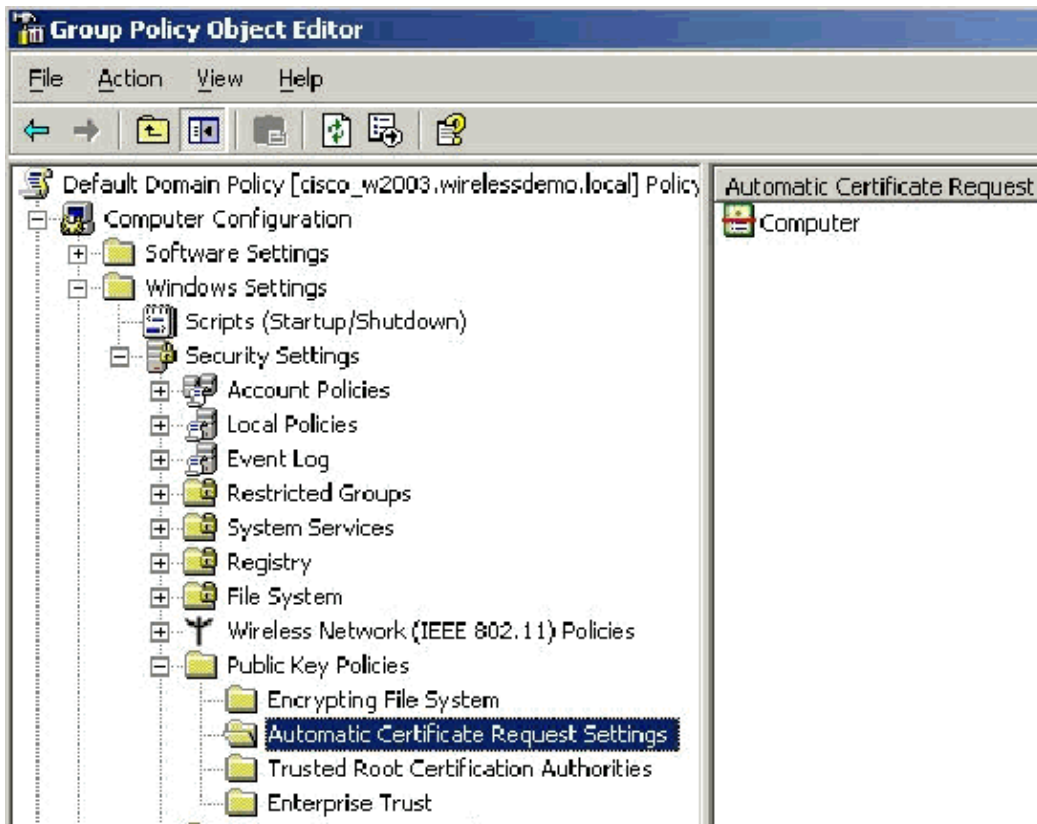


9. Right-click **Automatic Certificate Request Settings** and choose **New > Automatic Certificate Request**.
10. On the Welcome to the Automatic Certificate Request Setup Wizard page, click **Next**.
11. On the Certificate Template page, click **Computer** and click **Next**.

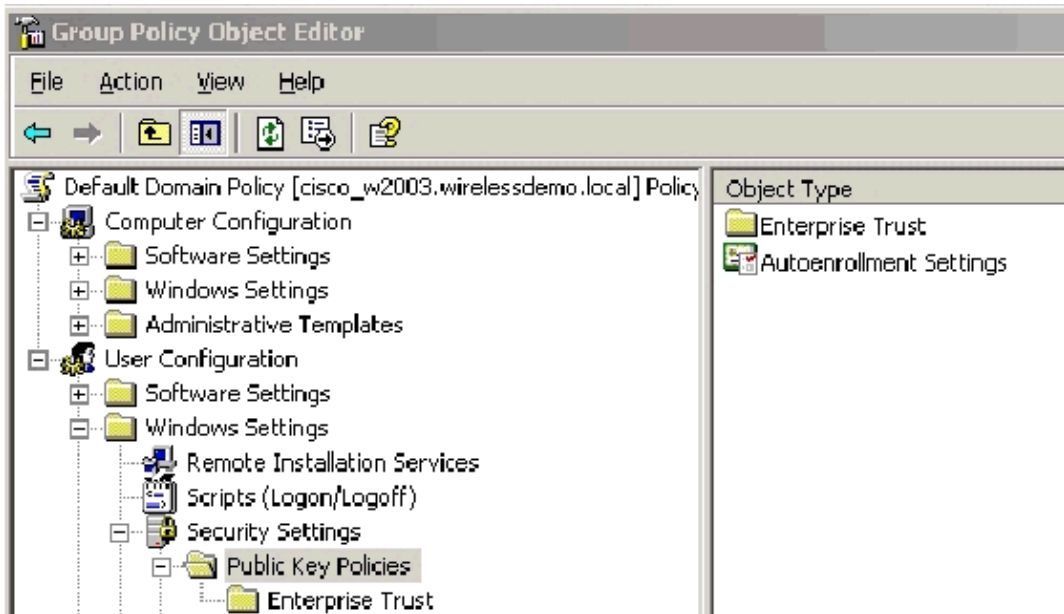


12. When you complete the Automatic Certificate Request Setup Wizard page, click **Finish**.

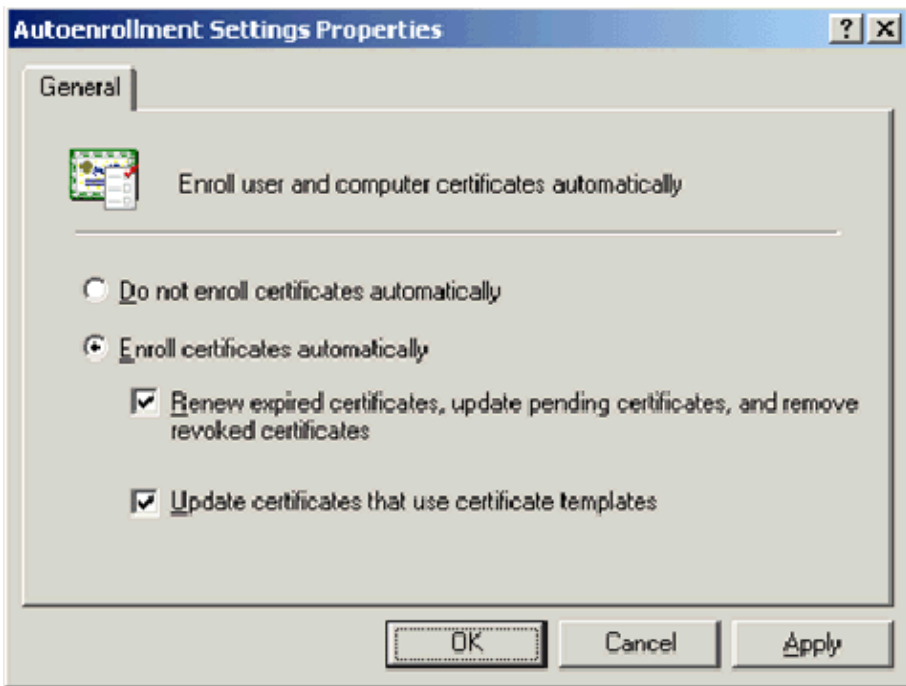
The Computer certificate type now appears in the details pane of the Group Policy Object Editor snap-in.



13. In the console tree, expand **User Configuration > Windows Settings > Security Settings > Public Key Policies**.



14. In the details pane, double-click **Autoenrollment Settings**.
15. Choose **Enroll certificates automatically** and check **Renew expired certificates, update pending certificates and remove revoked certificates** and **Update certificates that use certificate templates**.



16. Click **OK**.

## ACS 4.0 Certificate Setup

### Configure Exportable Certificate for ACS

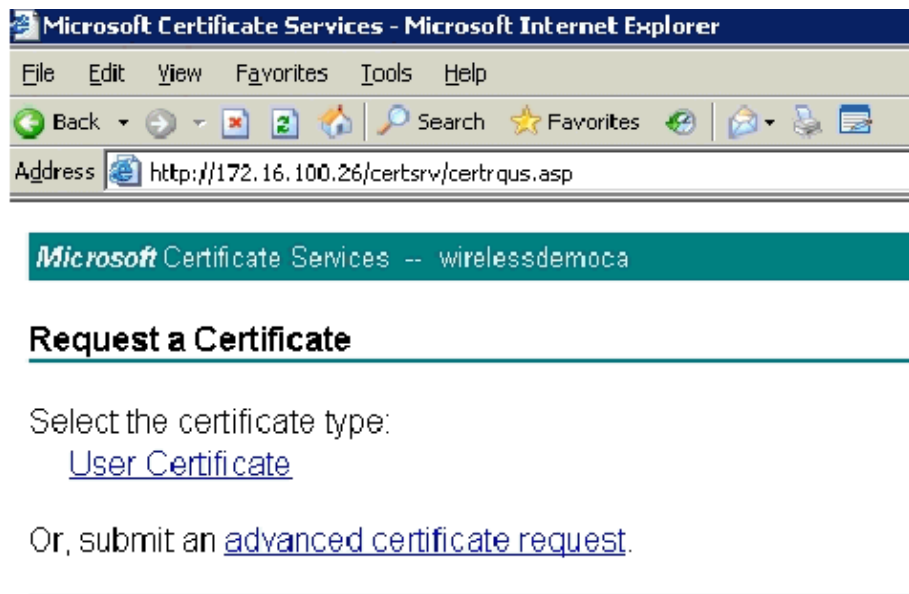
**Important:** The ACS server must obtain a server certificate from the enterprise root CA server in order to authenticate a WLAN PEAP client.

**Important:** Ensure that the IIS Manager is not open during the certificate setup process as causes problems with cached information.

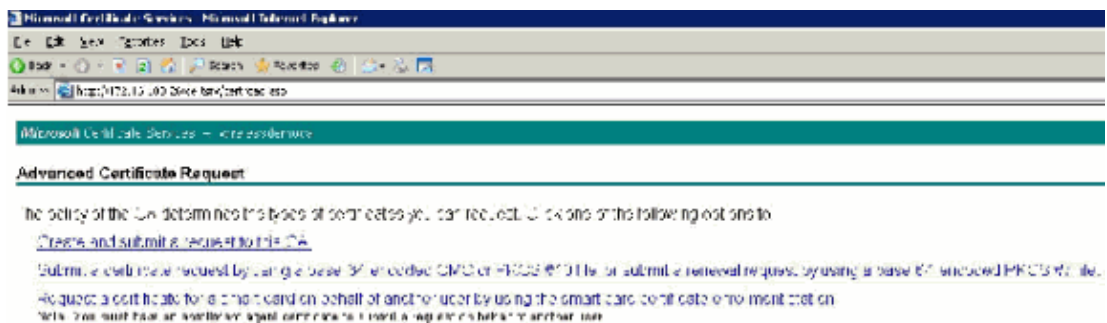
1. Log into the ACS server with an account that has Enterprise Admin rights.
2. On the local ACS machine, point the browser at the Microsoft certification authority server at **http://IP-address-of-Root-CA/certsrv**. In this case, the IP address is **172.16.100.26**.
3. Log in as the **Administrator**.



4. Choose **Request a Certificate** and click **Next**.



5. Choose **Advanced Request** and click **Next**.



6. Choose **Create and submit a request to this CA** and click **Next**.

**Important:** The reason for this step is due to the fact that Windows 2003 does not allow for exportable keys and you need to generate a certificate request based on the ACS Certificate that you created earlier that does.

Microsoft Certificate Services - wirelessdemo.local

### Advanced Certificate Request

Certificate Template: Administrator

Key Options:

Key Usage: Basic CFS

Key Length: 1024 bits

CSP: Wireless User Certificate Template

Key Usage: Store Certificate in the local computer certificate store

Key Store: Wireless User Certificate Template

Key Length: 1024 bits

Automatic key container name:  User specified key container name:

Mark keys as exportable:

Export keys to file:

Enable strong private key protection:

Store certificate in the local computer certificate store:

Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format:  CMC  PKCS10

Hash Algorithm: SHA-1

Only used to sign request.

Save request to file:

Expiration:

Friendly Name:

Submit >

- From the Certificate Templates select the certificate template created earlier named **ACS**. The options change after you select the template.
- Configure the **Name** to be the fully qualified domain name of the ACS server. In this case the ACS server name is cisco\_w2003.wirelessdemo.local. Ensure that **Store certificate in the local computer certificate store** is checked and click **Submit**.

Microsoft Certificate Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Deck Search Favorites

Address http://172.16.100.25/certsrv/cestrgna.asp

---

**Certificate Template:**

ACS

---

**Identifying Information For Offline Template:**

Name:

E-Mail:

Company:

Department:

City:

State:

Country/Region:

---

**Key Options:**

Create new key set  Use existing key set

CSP:

Key Usage:  Exchange

Key Size:  Min: 1024 Max: 1024 (common key sizes: 3072)

Automatic key container name  User specified key container name

Mark keys as exportable

Export keys to file

Store certificate in the local computer certificate store  
Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

---

**Additional Options:**

Request Format:  CMC  PKCS#10

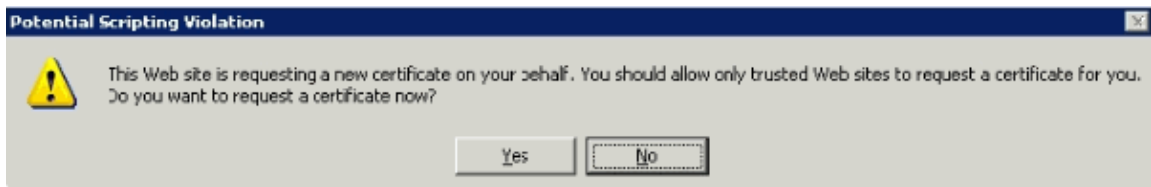
Hash Algorithm:   
Only used to sign request.

Save request to a file

Attributes:

Friendly Name:

9. A pop up window appears warning about a potential scripting violation. Choose **Yes**.



10. Click **Install this certificate**.



Microsoft Certificate Services -- wirelessdemoca

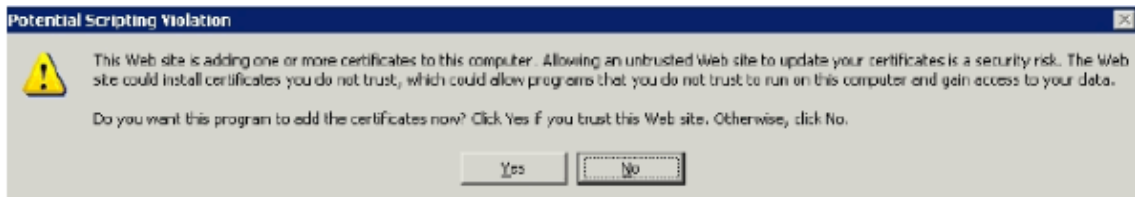
## Certificate Issued

The certificate you requested was issued to you.

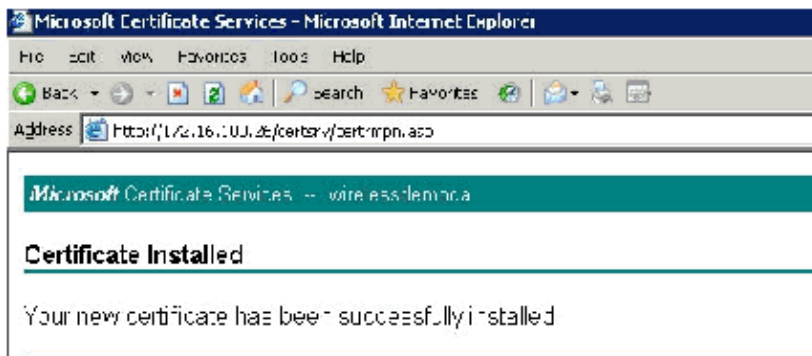


[Install this certificate](#)

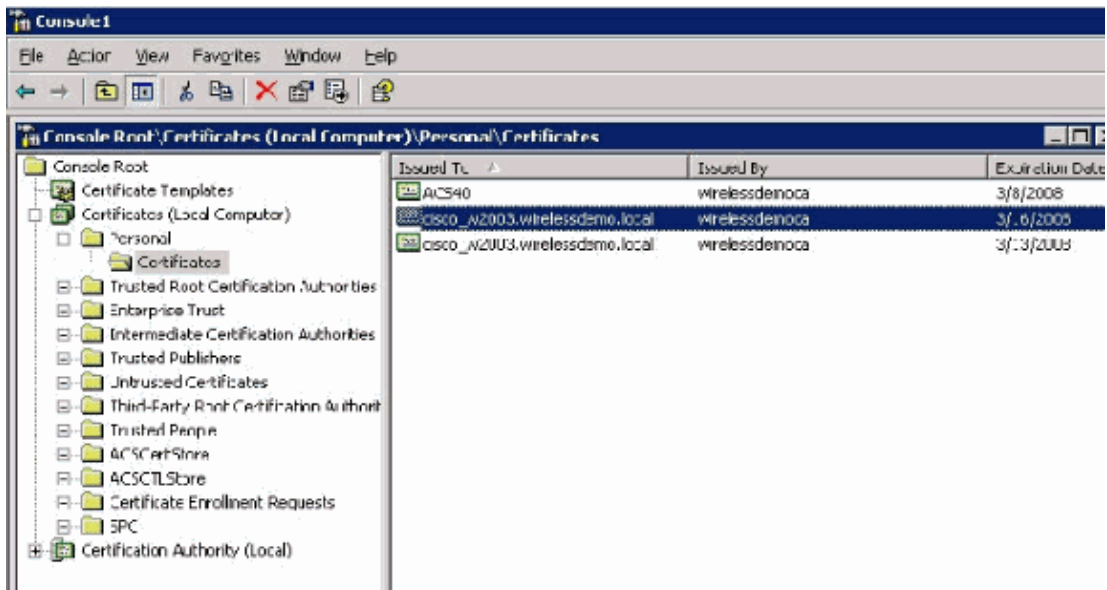
11. A pop up window appears again and warns about a potential scripting violation. Choose Yes.



12. After you click **Yes**, the certificate is installed.



13. At this point, the certificate is installed in the Certificates MMC under **Personal > Certificates**.

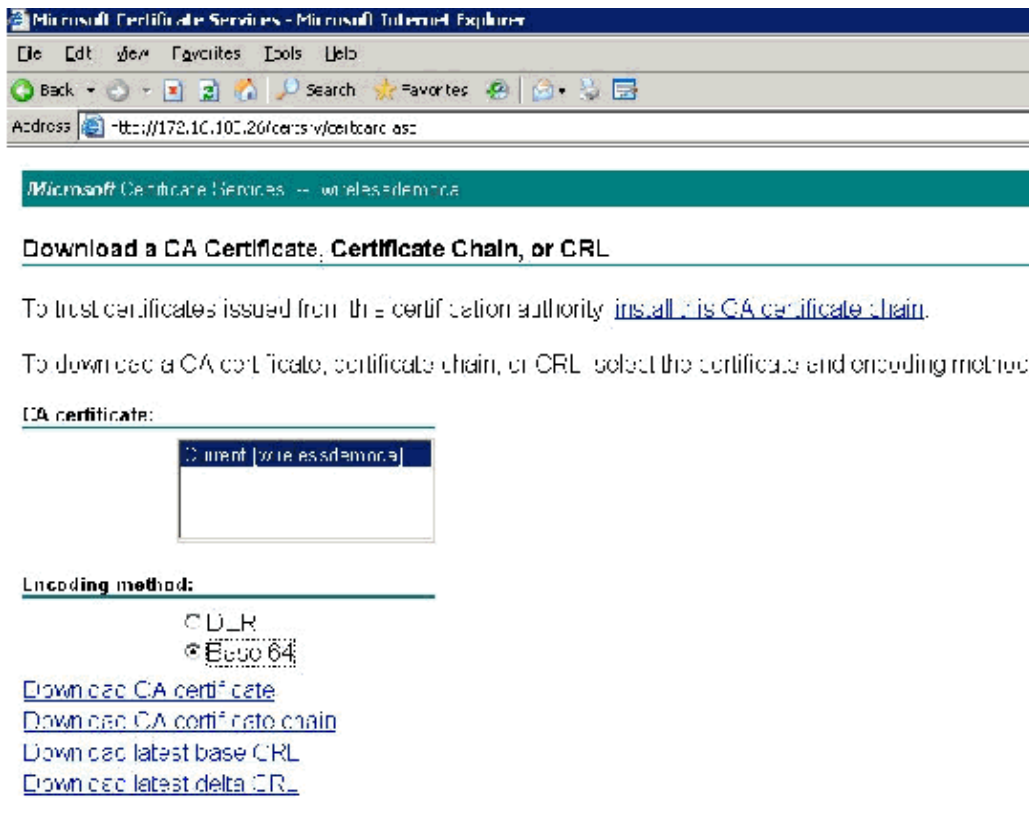


- Now that the certificate is installed to the local computer (ACS or cisco\_w2003 in this example), you need to generate a certificate file (.cer) for the ACS 4.0 certificate file configuration.
- On the ACS server (cisco\_w2003 in this example), point the browser at the Microsoft Certification Authority server to **http://172.16.100.26 /certsrv**.

## Install the Certificate in ACS 4.0 Software

Complete these steps:

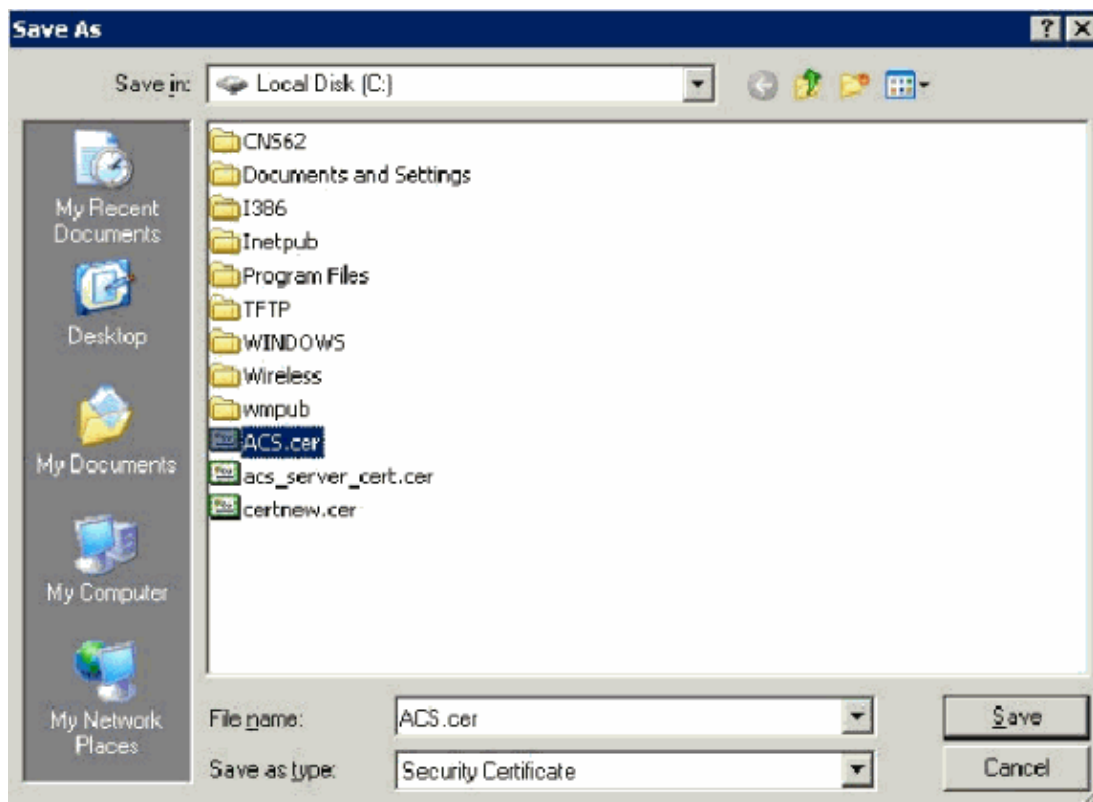
- On the ACS server (cisco\_w2003 in this example), point the browser at the Microsoft CA server to **http://172.16.100.26 /certsrv**.
- From the Select a Task option choose **Download a CA certificate, certificate chain or CRL**.
- Choose the **Base 64** radio encoding method and click **Download CA Certificate**.



4. A File Download Security Warning window appears. Click **Save**.

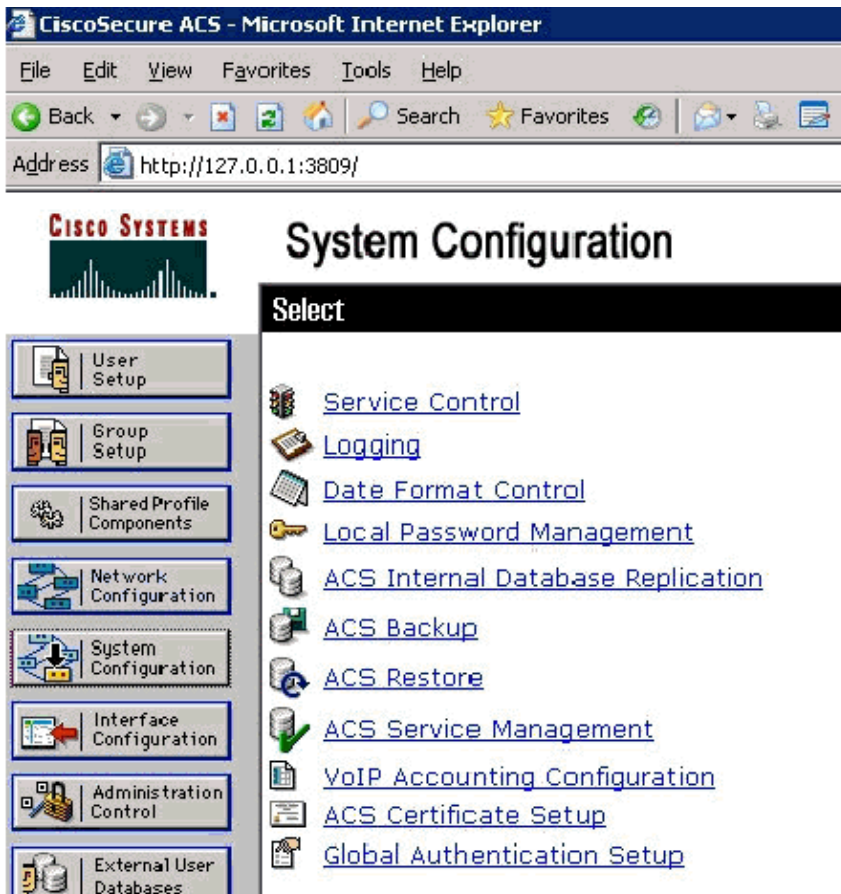


5. Save the file with a name such as ACS.cer or any name that you wish. Remember this name since you use it during the ACS Certificate Authority setup in ACS 4.0.

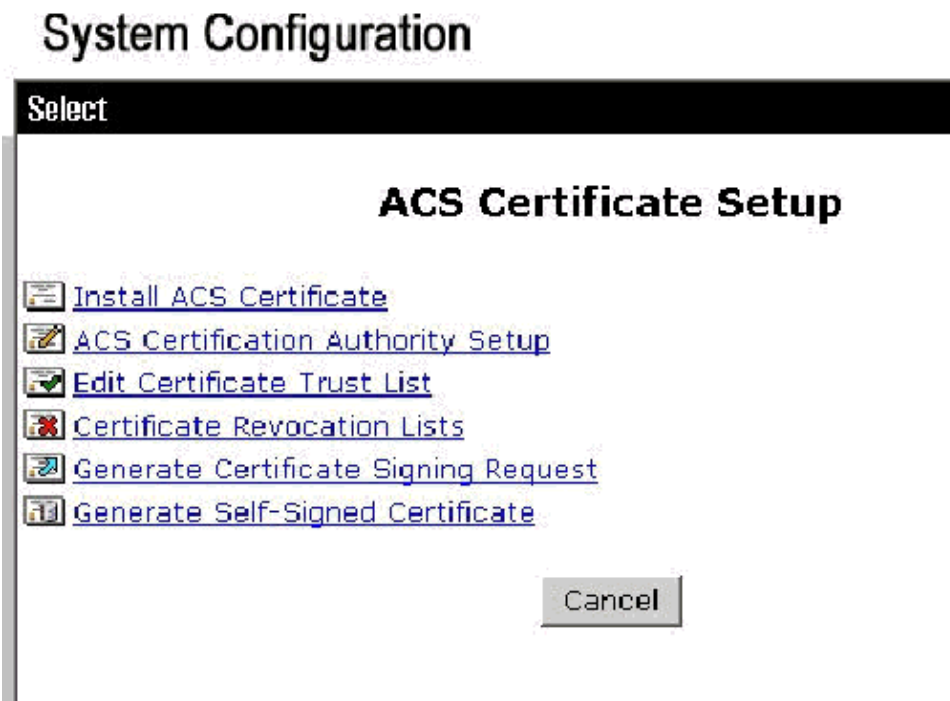


6. Open **ACS Admin** from the desktop shortcut created during the installation.

7. Click **System Configuration**.



8. Click **ACS Certificate Setup**.




9. Click **Install ACS Certificate**.

**System Configuration**

**Edit**

**Install ACS Certificate**

**Install new certificate** 

Read certificate from file

**Certificate file**

Use certificate from storage

**Certificate CN**

**Private key file**

**Private key password**

10. Choose **Use certificate from storage** and type in the fully qualified domain name of **cisco\_w2003.wirelessdemo.local** (or ACS.wirelessdemo.local if you used ACS as the name).

**System Configuration**

**Edit**

**Install ACS Certificate**

**Install new certificate** 

Read certificate from file

**Certificate file**

Use certificate from storage

**Certificate CN**

**Private key file**

**Private key password**

11. Click **Submit**.

# System Configuration

Edit

## Install ACS Certificate

### Installed Certificate Information


<b>Issued to:</b>	cisco_w2003.wirelessdemo.local
<b>Issued by:</b>	wirelessdemoca
<b>Valid from:</b>	March 17 2006 at 08:33:25
<b>Valid to:</b>	March 16 2008 at 08:33:25
<b>Validity:</b>	OK


**The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.**


12. Click **System Configuration**.
13. Click **Service Control** and then click **Restart**.

# System Configuration

Select

CiscoSecure ACS on cisco_w2003 
<b>Is Currently Running</b>


<b>Services Log File Configuration</b> 
Level of detail <input type="radio"/> None <input checked="" type="radio"/> Low <input type="radio"/> Full
Generate New File <input checked="" type="radio"/> Every day <input type="radio"/> Every week <input type="radio"/> Every month <input type="radio"/> When size is greater than <input type="text" value="2048"/> KB
<input type="checkbox"/> Manage Directory <input type="radio"/> Keep only the last <input type="text" value="7"/> files <input checked="" type="radio"/> Delete files older than <input type="text" value="7"/> days

 [Back to Help](#)

14. Click **System Configuration**.
15. Click **Global Authentication Setup**.
16. Check **Allow EAP-MSCHAPV2** and **Allow EAP-GTC**.

# System Configuration

## Global Authentication Setup

EAP Configuration 

**PEAP**

Allow EAP-MSCHAPV2

Allow EAP-GTC

Allow Posture Validation

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

---

**EAP-FAST**

[EAP-FAST Configuration](#)

---

**EAP-TLS**

Allow EAP-TLS

Select one or more of the following options:

- Certificate SAN comparison
- Certificate CN comparison
- Certificate Binary comparison

EAP-TLS session timeout (minutes):

17. Click **Submit + Restart**.
18. Click **System Configuration**.
19. Click **ACS Certification Authority Setup**.
20. Under the ACS Certification Authority Setup window, type the name and location of the \*.cer file created earlier. In this example, the \*.cer file created is **ACS.cer** in the root directory c:\.
21. Type **c:\acs.cer** in the CA certificate file field and click **Submit**.

## System Configuration

**ACS Certification Authority Setup**

CA Operations

Add new CA certificate to local certificate storage

CA certificate file

System Configuration

**ACS Certification Authority Setup**

CA Operations

Add new CA certificate to local certificate storage

CA certificate file

New CA certificate is successfully added into the global system certificate storage.

CA certificate common name	wirelessdemo.ca
----------------------------	-----------------

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

22. Restart the ACS service.

## CLIENT Configuration for PEAP using Windows Zero Touch

In our example, CLIENT is a computer that runs Windows XP Professional with SP that acts as a wireless client and obtains access to Intranet resources through the wireless AP. Complete the procedures in this section in order to configure CLIENT as a wireless client.

### Perform a Basic Installation and Configuration

Complete these steps:

1. Connect CLIENT to the Intranet network segment using an Ethernet cable connected to the hub.
2. On CLIENT, install Windows XP Professional with SP2 as a member computer named CLIENT of the wirelessdemo.local domain.
3. Install Windows XP Professional with SP2. This must be installed in order to have PEAP support.

**Note:** Windows Firewall is automatically turned on in Windows XP Professional with SP2. Do not turn the firewall off.

### Install the Wireless Network Adapter

Complete these steps:

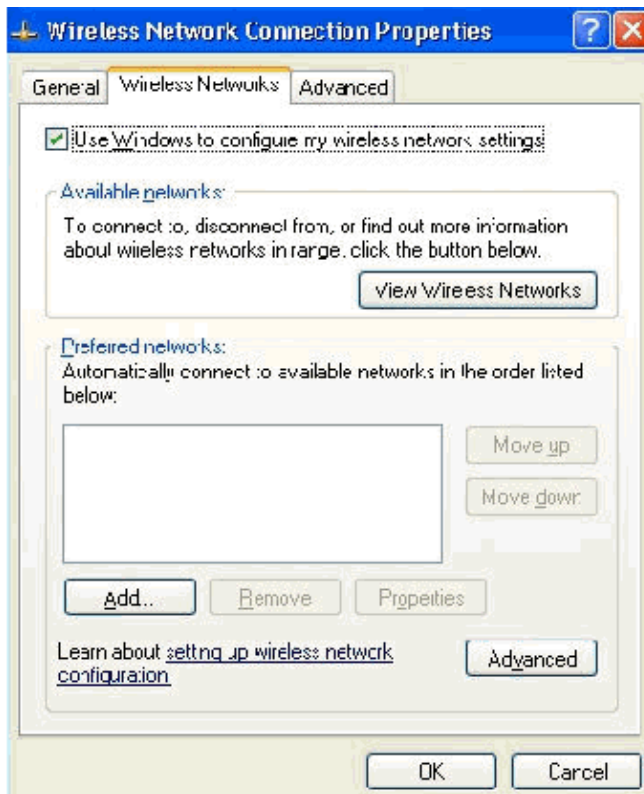
1. Shut down the CLIENT computer.
2. Disconnect the CLIENT computer from the Intranet network segment.
3. Restart the CLIENT computer, and then log on using the local administrator account.
4. Install the wireless network adapter.

**Important:** Do not install the manufacturer's configuration software for the wireless adapter. Install the wireless network adapter drivers using the Add Hardware Wizard. Also, when prompted, provide the CD provided by the manufacturer or a disk with updated drivers for use with Windows XP Professional with SP2.

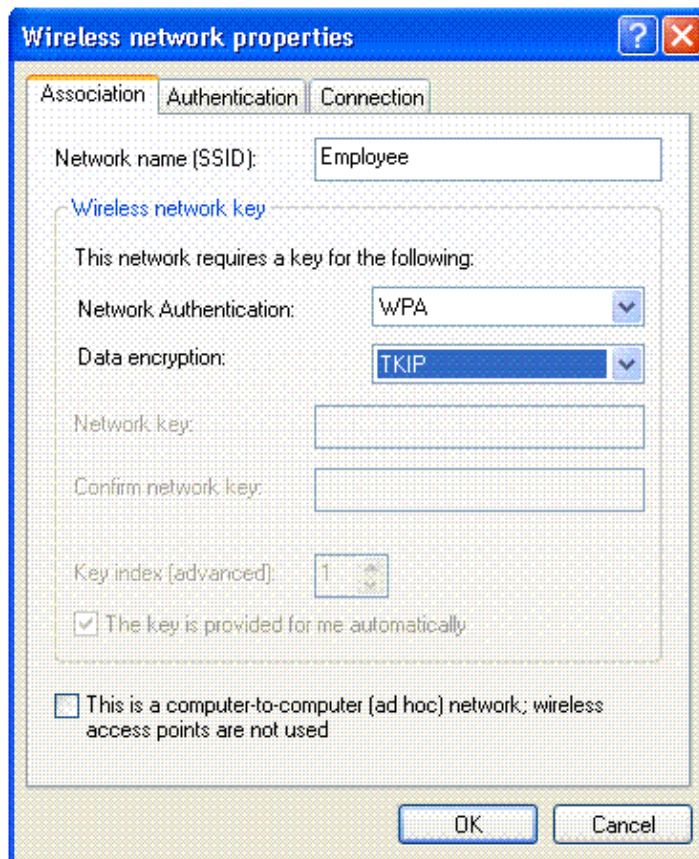
## Configure the Wireless Network Connection

Complete these steps:

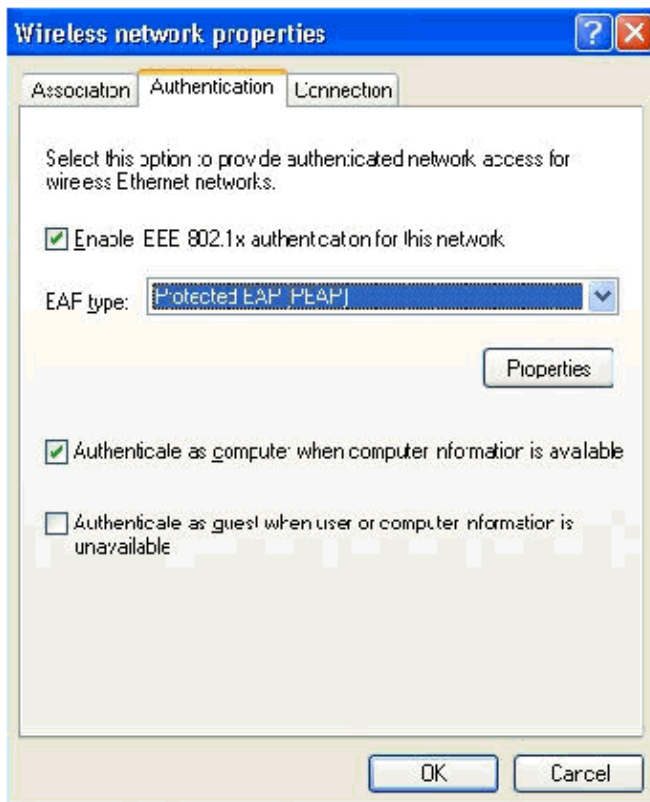
1. Log off and then log on by using the WirelessUser account in the wirelessdemo.local domain.
2. Choose **Start > Control Panel**, double-click **Network Connections**, and then right-click **Wireless Network Connection**.
3. Click **Properties**, go to the Wireless Networks tab, and ensure that the **Use Windows to configure my wireless network settings** is checked.



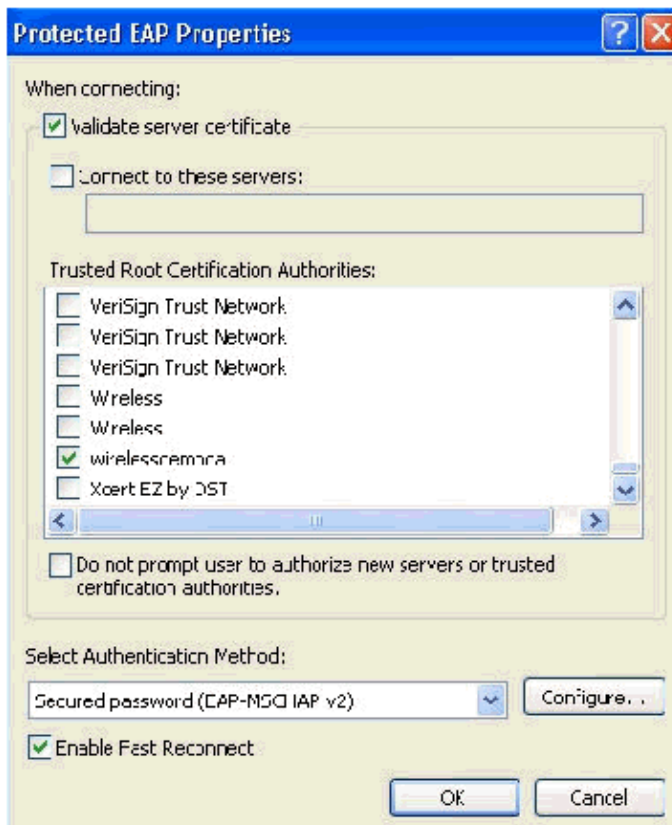
4. Click **Add**.
5. Under the Association tab, type **Employee** in the Network name (SSID) field.
6. Select **WPA** for the Network Authentication and ensure that Data Encryption is set to **TKIP**.



7. Go to the Authentication tab.
8. Validate that EAP type is configured to use **Protected EAP (PEAP)**. If it is not, select it from the drop-down menu.
9. If you want the machine to be authenticated prior to login (which allows login scripts or group policy pushes to be applied) check **Authenticate as computer when computer information is available**.

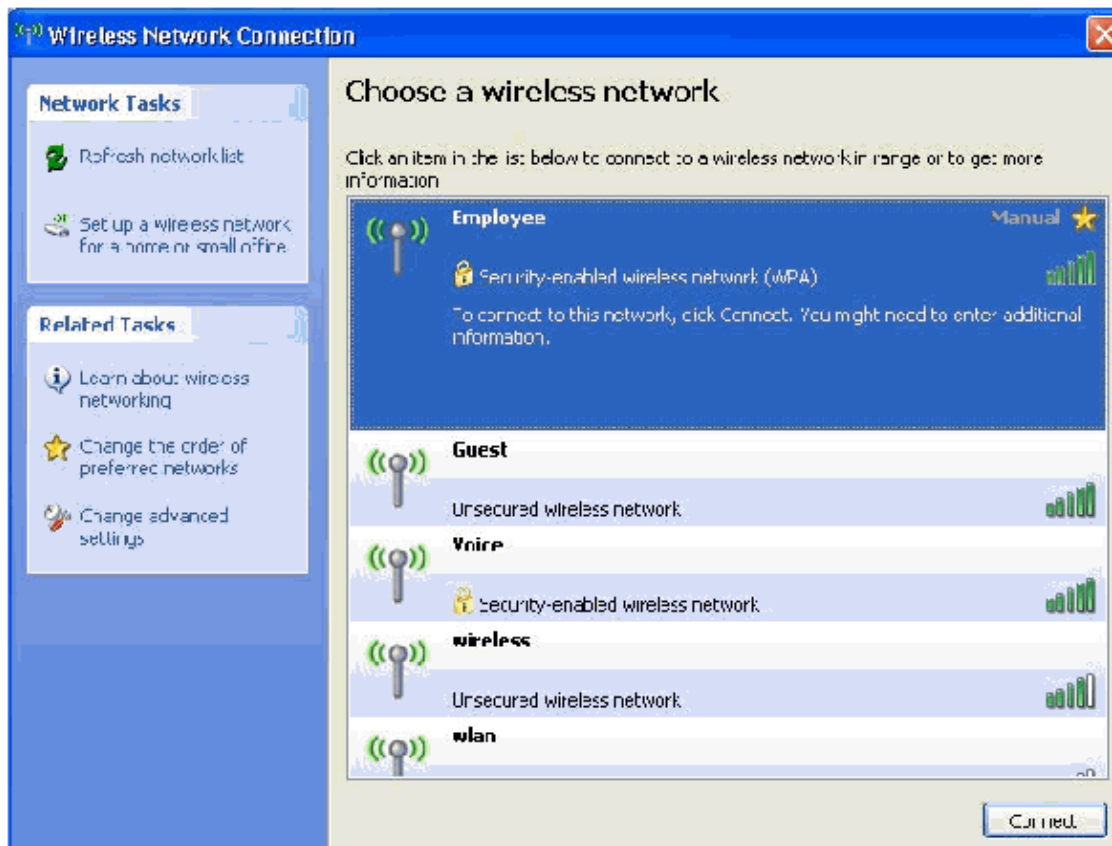


10. Click **Properties**.
11. As PEAP involves authentication of Server by the client ensure that Validate server certificate is checked. Also, make sure the CA that issued the ACS certificate is checked under the *Trusted Root Certification Authorities* menu.
12. Choose **Secured password (EAP-MSCHAP v2)** under Authentication Method as it is used for inner authentication.

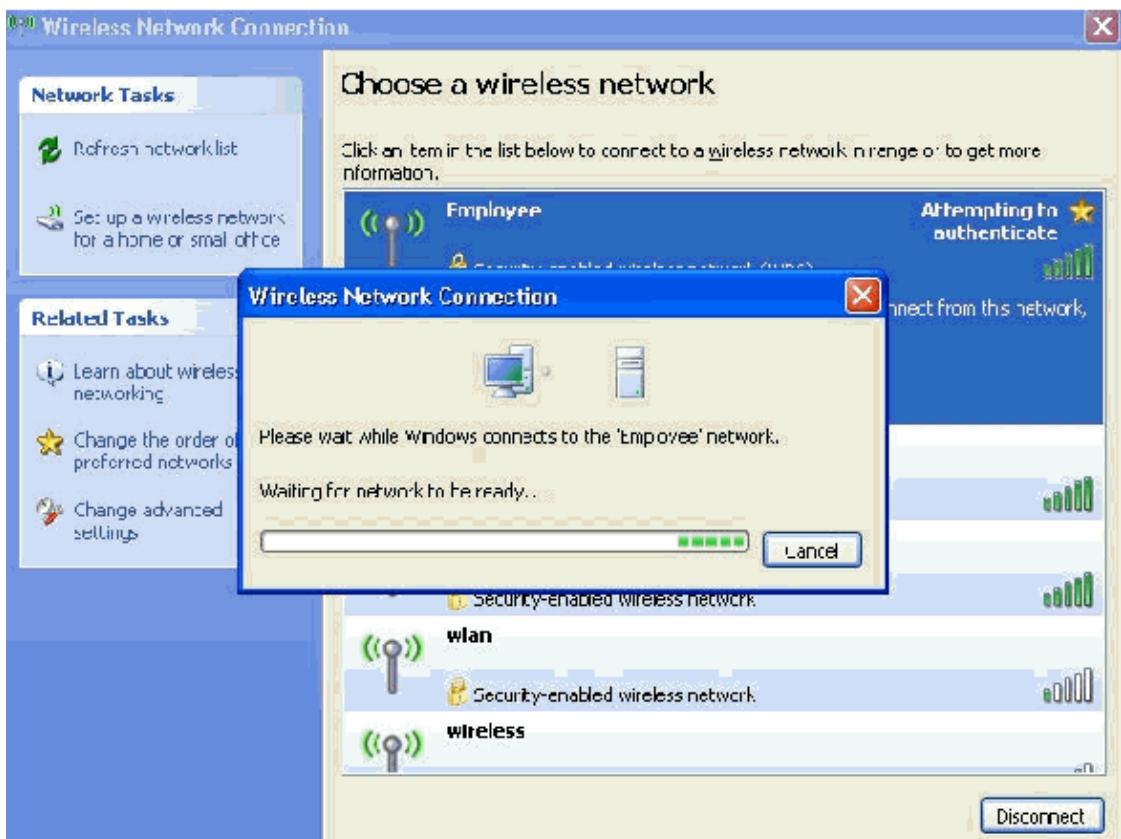
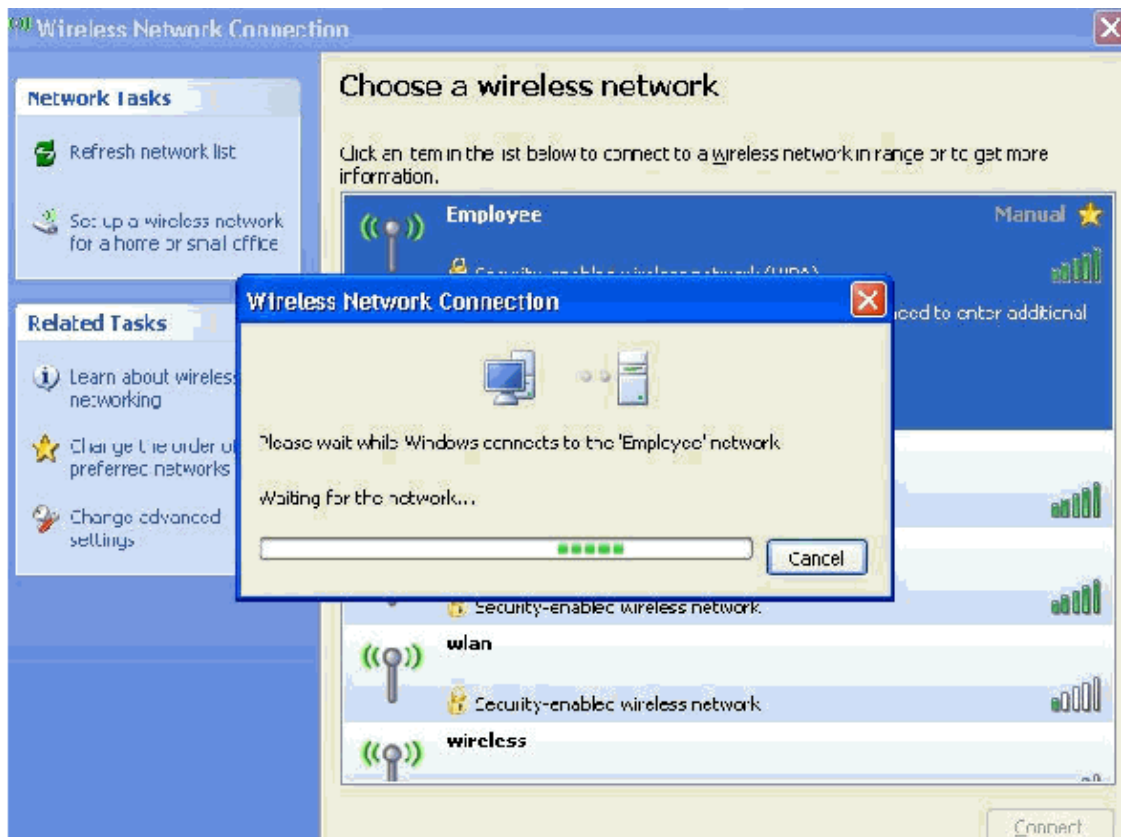


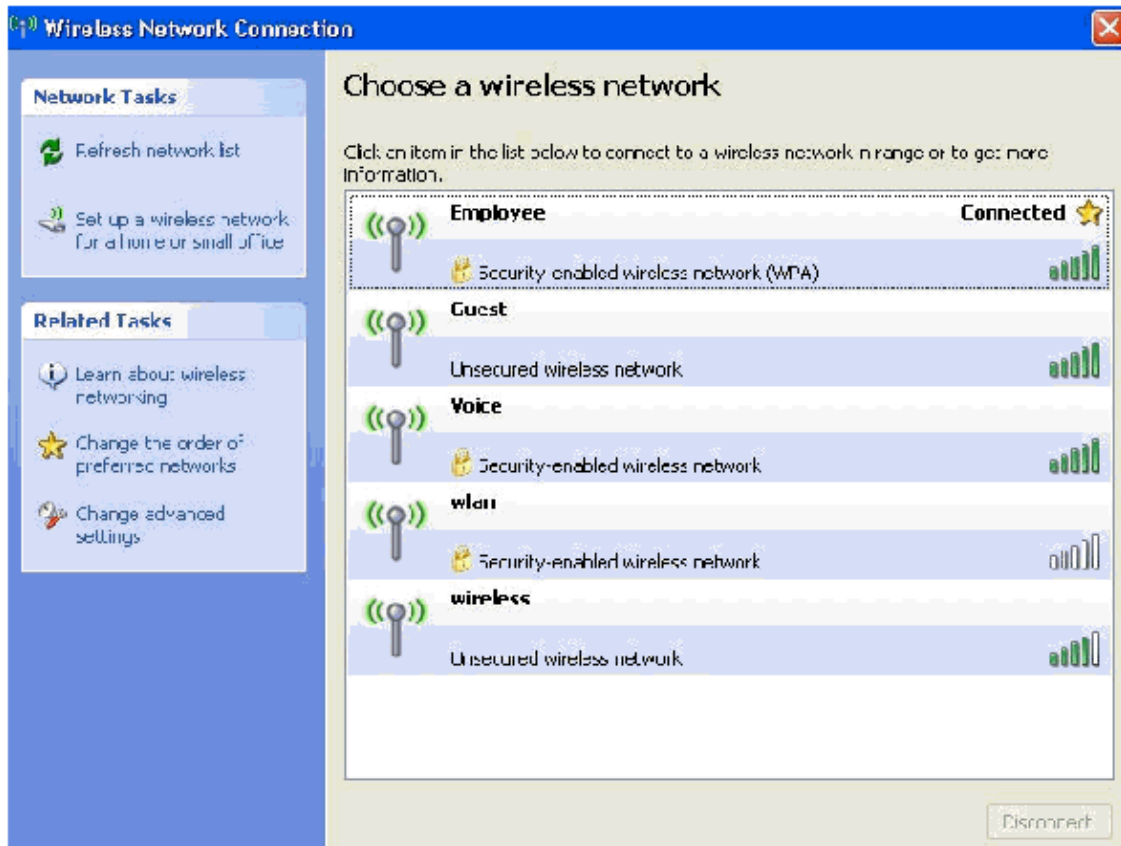
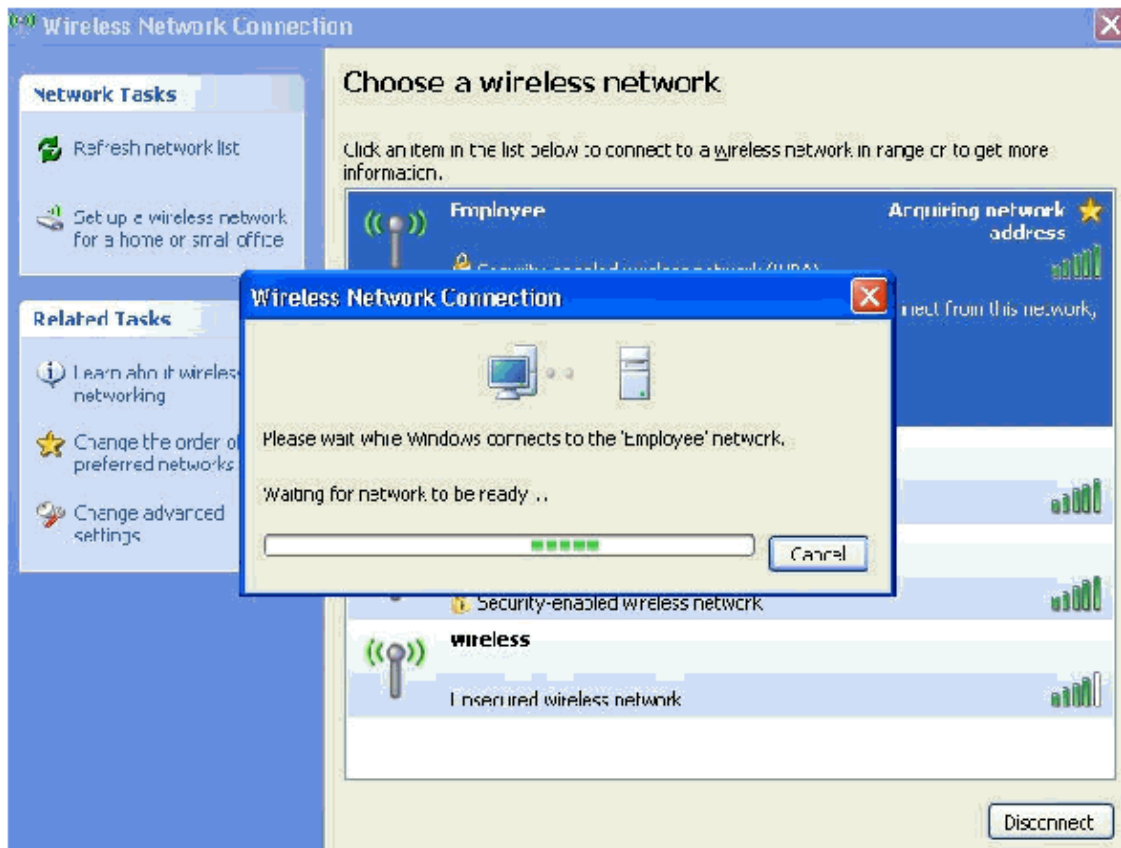
13. Make sure the Enable Fast Reconnect check box is checked. Then, click **OK** three times.

14. Right-click the wireless network connection icon in systray and then click **View Available Wireless Networks**.
15. Click the **Employee** wireless network and click **Connect**.



These screen shots indicate if the connection completes successfully.





16. After authentication is successful, check the TCP/IP configuration for the wireless adapter by using Network Connections. It should have an address range of 172.16.100.100–172.16.100.254 from the DHCP scope or the scope created for the wireless clients.
17. In order to test functionality, open up a browser and browse to <http://wirelessdemoca> (or the IP address of the Enterprise CA server).

## Problem: Odyssey Client Prompts Three Times for Token Authentication Platform

This issue occurs in all Windows versions and 2.x Solution.

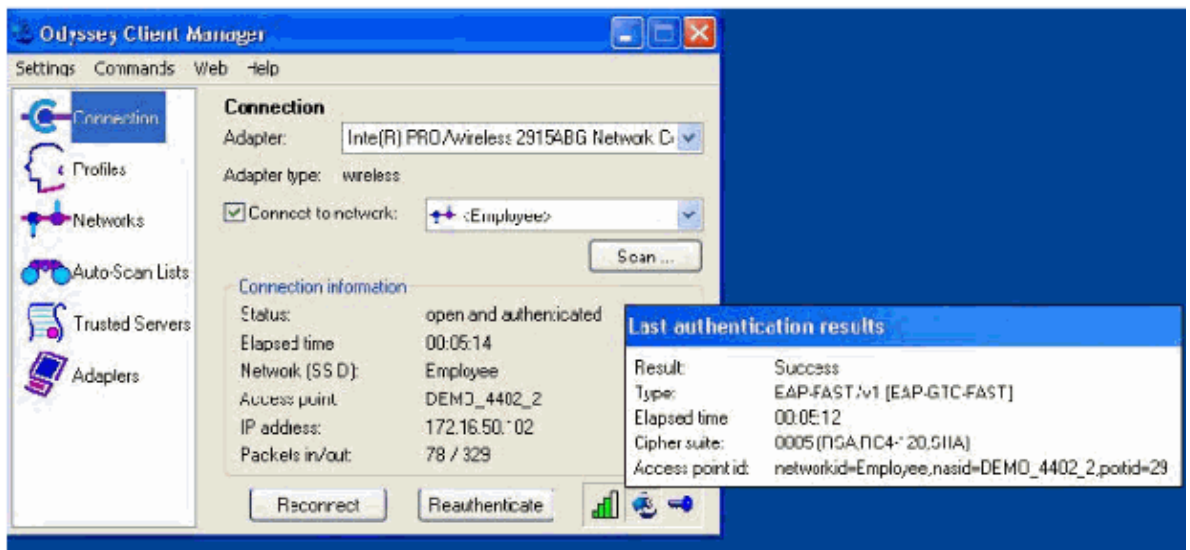
Typically, a wireless services setting in XP causes this to happen.

Complete these steps in order to correct this issue:

1. Choose **Start > Settings > Control Panel > Administrative Tools > Services**.
2. Go to the bottom of the list and look for **Wireless Zero Configuration**.
3. Double-click this setting.
4. Select the option to stop this service.
5. Under the setting for startup type select **disable**.

**Note:** If all you do is stop the service, it starts again on reboot, so you must disable it in order for this issue to not occur again.

6. Save the settings and close.



## PEAP Authentication Fails with ACS Server

When your client fails PEAP authentication with an ACS server, check if you find the *"NAS duplicated authentication attempt"* error message in the **Failed attempts** option under the **Report and Activity** menu of the ACS.

You might receive this error message when Microsoft Windows XP SP2 is installed on the client machine and Windows XP SP2 authenticates against a third party server other than a Microsoft IAS server. In particular, Cisco RADIUS server (ACS) uses a different method to calculate the Extensible Authentication Protocol Type:Length:Value format (EAP-TLV) ID than the method Windows XP uses. Microsoft has identified this as a defect in the XP SP2 supplicant.

For a Hotfix, contact Microsoft and refer to article KB885453. The underlying issue is that on the client side, with *windows utility*, the **Fast Reconnect** option is disabled for PEAP by default. However, this option is enabled by default on the server side (ACS). In order to resolve this issue, uncheck the **Fast Reconnect** option on the ACS server and press **submit+restart**. Alternatively, you can enable the Fast Reconnect option on the client side to resolve the issue.

Complete these steps in order to enable Fast Reconnect on the client that runs Windows XP using Windows Utility:

1. Click **Start > Settings > Control Panel**.
2. Double click the **Network Connections** icon.
3. Right click the **Wireless Network Connection** icon and click **Properties**.
4. Click the **Wireless Networks** tab.
5. Check the *Use Windows to configure my wireless network settings* option to enable windows to configure the client adapter.
6. If you have already configured an SSID, choose the SSID and click **Properties**. If not, click *New* to add a new WLAN.
7. Enter the SSID under the **Association** tab. Make sure that *Network Authentication* is **Open** and *Data Encryption* is set to **WEP**.
8. Click **Authentication**.
9. Check the *Enable IEEE 802.1x authentication for this network* option.
10. Choose the *EAP Type* as **PEAP** and click **Properties**.
11. Check the **Enable Fast Reconnect** option at the bottom of the page.



---

## Related Information

- [EAP Authentication with WLAN Controllers \(WLC\) Configuration Example](#)
- [Wireless LAN Controller Configuration Guide](#)
- [Wireless LAN Controller and Lightweight Access Point Basic Configuration Example](#)
- [VLANs on Wireless LAN Controllers Configuration Example](#)
- [AP Group VLANs with wireless LAN Controllers Configuration Example](#)
- [Technical Support & Documentation – Cisco Systems](#)

